JULGEOLEKUASUTUSTE TEGEVUSE REGULATSIOONI VÕRDLEV ANALÜÜS

17.01.2017

Sisukord

1. SISSEJUHATUS

Julgeoleku- ja luureasutuste volitused ning nende kasutuses olevad meetmed[1] on riigiti reguleeritud erinevalt. Eesti õigusloome praktikas on julgeoleku- ja luureasutuste õigusi ja meetmeid reguleerivaid õigusakte muudetud pigem *ad hoc* ning konkreetsete juhtumite ja vajaduste põhiselt. Juhtumipõhise õigusloome suurimaks probleemiks on aga regulatsiooni üha suurenev killustatus ning selgetest põhimõtetest lähtuva strateegilise suuna puudumine.

Selleks, et kujundada sisejulgeolekupoliitikat ning kriminaalpoliitikat, hinnata kooskõlastamiseks esitatud ettepanekuid ning algatada ja toetada julgeolekuasutuste tegevusega seotud õigusloomet, on vajalik omada ülevaadet teiste riikide praktikast.

Käesoleva uuringu eesmärgiks on anda ülevaade Eesti, Rootsi, Soome, Ühendkuningriigi, Hollandi ning Saksamaa julgeoleku- ja luureasutuste tegevusele kohalduvast regulatsioonist. Käesoleva uuringuga antakse ülevaade nende riikide julgeoleku- ja luureasutuste volitustest ja meetmetest, põhiõiguste riive õiguspärasuse tagamise protseduuridest ja kontrollimehhanismidest, läbivatest põhimõtetest julgeoleku- ja luureasutuste tegevuse reguleerimisel ning volituste ja meetmete arendamisel. Lisaks on uuringu eesmärgiks anda võrdlev ülevaade, millised on uuringusse kaasatud riikide regulatsioonide sarnasused ja erinevused võrreldes Eestis kehtiva regulatsiooniga.

Käesoleva uuringuga kaardistatakse julgeoleku- ja luureasutuste tegevust reguleerivad õigusaktid ja pädevad asutused ning tuuakse iga riigi puhul välja:

1) julgeoleku- ja luureasutuste peamised ülesanded;
2) julgeoleku- ja luureasutuste peamised volitused (nt sõnumisaladuse piiramine, kodu, perekonna- või eraelu puutumatuse õiguse piiramine) ning meetmed (erinevad teabekogumise meetmed, erinevad uurimis- ja jälitustoimingud, nt varjatud jälgimine, pealtkuulamine, kuriteo matkimine, variandmete kasutamine, konspiratsioonivõtted, krüpteeritud andmete avamine, tegutsemine välisriigis jne);
3) põhiõiguste riive õiguspärasuse tagamise protseduurid (eelkõige *ex ante* kontrollimehhanismid);
4) järelevalve korraldus julgeoleku- ja luureasutuste tegevuse õigus- ja eesmärgipärasuse üle (*ex post* kontrollimehhanismid);
5) julgeoleku- ja luureasutuste volitused ja meetmed elektroonilise side jälgimisel ning andmete töötlemisel ja talletamisel;
6) järeldused läbivate regulatsiooni üldpõhimõtete kohta.

Igat riiki käsitletakse eraldi peatükis, mis sisaldab eelnimetatud komponente. Soome, Rootsi, Ühendkuningriigi, Hollandi ning Saksamaa peatükid sisaldavad ka võrdlust Eestiga.

Lisaks tekstilisele kirjeldusele on võrdleva analüüsi lisades ülevaatlikud tabelid riikide kehtivate regulatsioonide võrdluse kohta.

Uuringu metoodika

Uuringuga hõlmatud riigid valiti lähtuvalt järgmistest põhimõtetest. Saksamaa on valitud põhjusel, et Saksa õigussüsteem on kõige sarnasem Eesti õigussüsteemiga. Ühendkuningriik valiti tulenevalt Ühendkuningriigi pikaaegsest kogemusest ja juhirollist julgeolekuasutuste tegevuse reguleerimisel demokraatlikus õigusriigis. Soome, Rootsi ja Holland on valitud põhjusel, et valitud riikide seas oleksid esindatud nii sõjaliselt neutraalsed Põhjamaad kui ka Põhja-Atlandi Lepingu Organisatsiooni kuuluvad riigid, mis kuuluksid ühtlasi nende riikide hulka, kus põhiõiguste kaitse on väga heal tasemel[2].

[1] Käesolevas uuringus kasutatakse terminit „meede“ (abinõu) erinevate julgeoleku- ja luureasutuste tegevuse puhul (nt varjatud jälgimine, pealtkuulamine, kuriteo matkimine jne). Eesti ja teiste riikide õiguses ei ole selgelt eristatud meetmeid ja meetodeid. Näiteks JAS § 21 lg 3 räägib meetme rakendamisest, JAS § 28 meetodist. Põhiõiguste kontekstist lähtuvalt on sobilikum rääkida meetmetest.

[2] World Justice Project Rule of Law 2016 indeksi järgi on põhiõiguste kaitse valdkonnas Soome 2. kohal, Rootsi 5. kohal ning Holland 6. kohal (võrdluseks: Eesti on 15. kohal)
http://worldjusticeproject.org/sites/default/files/media/wjp_rule_of_law_index_2016.pdf

Käesoleva võrdleva analüüsi läbiviimiseks kasutati õigusliku analüüsi meetodeid, sh kvalitatiivset sisuanalüüsi, mis hõlmas dokumendianalüüsi ja võrdlevat õigusanalüüsi. Analüüsi oluliseks osaks oli kirjeldava ülevaate koostamine, mille põhjal koostati omakorda uuringusse kaasatud riikide võrdlus Eestis kehtiva regulatsiooniga.

Kuivõrd õigusanalüüsi koostamisel tugineti ka juba varasemalt teostatud õigusanalüüsidele (sh Eestis ja teistes riikides teostatud uuringutele, juhenditele, soovitustele), rakendati õigusanalüüsi koostamisel meta-analüüsi, st analüüsiti varasemate uurimuste tulemusi.

Samuti pöörati tähelepanu regulatsiooni keskmes olevate mõistete defineerimisele, eelkõige julgeoleku- ja luureasutuste kasutatavate meetmete osas. Järeldused läbivatest põhimõtetest julgeoleku- ja luureasutuste tegevuse reguleerimisel ning elluviimisel tehti induktiivse analüüsi vormis.

Uuringu koostas Advokaadibüroo Sorainen AS.

Allar Jõks
vandeadvokaat

Piret Schasmin
vandeadvokaadi abi

2. LÜHIKOKKUVÕTE UURINGU TULEMUSTEST

Käesoleva uuringu eesmärgiks oli anda ülevaade Eesti, Soome, Rootsi, Ühendkuningriigi, Hollandi ning Saksamaa julgeoleku- ja luureasutuste tegevusele kohalduvast regulatsioonist. Käesoleva uuringuga anti ülevaade nende riikide julgeoleku- ja luureasutuste volitustest ja meetmetest, põhiõiguste riive õiguspärasuse tagamise protseduuridest ja kontrollimehhanismidest, läbivatest põhimõtetest julgeoleku- ja luureasutuste tegevuse reguleerimisel ning volituste ja meetmete arendamisel. Sealjuures analüüsiti, millised on uuringusse kaasatud riikide regulatsioonide sarnasused ja erinevused võrreldes Eestis kehtiva regulatsiooniga.

Käesolevas uuringus anti esmalt ülevaade Eesti julgeoleku- ja luureasutuste (Teabeameti, Kaitsepolitseiameti ning kaitseväeluuret teostava Kaitseväe) regulatsioonist. Eesti julgeoleku- ja luureasutuste tegevuse regulatsiooni iseloomustab killustatus väga paljude erinevate õigusaktide vahel, samuti õigusliku regulatsiooni ebaselgus nii sätete sisu kui ka erinevate õigusaktide koostoime osas. Eelkõige puudutab see Kaitsepolitseiametit, kellel on nii vastuluure, korrakaitse (sh riikliku järelevalve) kui ka süüteomenetluse (nii kriminaal- kui ka väärteomenetluse) funktsioonid, kuid ka Teabeametit puudutavale regulatsioonile saab ette heita ebaselgust. Näiteks ei ole piisavalt selgelt sõnastatud, milliste ülesannete täitmiseks võivad Teabeamet ja Kaitsepolitseiamet julgeolekuseaduse 4. peatükis sätestatud volitusi ning meetmeid kasutada (nt JAS § 26 lg-t 3). Samuti ei selgu julgeolekuasutuste seadusest otseselt, milliste tegevuste (kas vastuluure, korrakaitse või süütegude menetlemise) jaoks võib kohaldada politsei ja piirivalve seaduses sätestatud meetmeid.

Samuti kinnitab regulatsiooni ebaselgust, killustatust ning ühtse lähenemise puudust see, et korrakaitse ülesannete täitmisel võib Kaitsepolitseiamet lähtuda nii julgeolekuasutuste seadusest, kriminaalmenetluse seadustikust, korrakaitseseadusest kui ka politsei ja piirivalve seadusest. Sealjuures sätestatavad need seadused osaliselt samu meetmeid, kuigi protseduurid või põhimõtted nende kasutamiseks võivad erineda. Näiteks elektroonilise side meta-andmete päringu esitamiseks ei ole korrakaitseseaduse alusel eelnevat loa protseduuri, samas politsei ja piirivalve seaduse alusel muu kui omanikupäringu korral on nõutav prokuratuuri luba (võrdluseks ka julgeolekuasutuste seaduse alusel on vaja üksnes Kaitsepolitseiameti juhi või tema volitatud ametniku luba). Kuivõrd Kaitsepolitseiameti tegevus võib ühe eesmärgi nimel toimuda erinevatel alustel, on ebaselge, milline on eelnevalt nimetatud õigusaktide koostoime ning tõusetub küsimus, mille alusel otsustab Kaitsepolitseiamet, millisest seadusest oma tegevuses lähtuda.

Seejärel anti ülevaade Rootsi Kaitsepolitsei (Säkerhetspolisen, SÄPO) ning välisluurega tegelevate asutuste (Kaitsejõud (Försvarsmakten), Raadioluureamet (Försvarets Radioanstalt), Kaitsejõudude Relvastuse ja Kaitsetehnika Amet (Försvarets materielverk) ja Totaalkaitse Uurimisinstituut (Totalförsvarets forskningsinstitut)) regulatsioonist. Rootsi julgeoleku- ja luureasutuste tegevuse regulatsiooni iseloomustab killustatus erinevate õigusaktide vahel, samuti see, et välisluurega tegelevate asutuste rakendatavaid meetmeid ja nende rakendamise aluseid õigusaktides täpsemalt ei reguleerita, v.a Raadioluureameti osas.

Soome regulatsiooni ülevaates kirjeldati Kaitsepolitsei (Suojelupoliisi, SUPO) ja Kindralstaabi Luureosakonna (Pääesikunnan Tiedusteluosasto, PVTK) tegevuse õiguslikku raamistikku. SUPO ja PVTK tegevust reguleerivad seadused ühtlustati 2014. aastal toimunud reformi käigus, mistõttu on Soome regulatsioon mõlema asutuse puhul selge ning erinevate ülesannete täitmisel on meetmed, nende rakendamise tingimused ja protseduurid sarnased. Samas on seaduse tasemel jäetud SUPO konkreetsed ülesanded avatuks, jättes nende täpsustamise vastavalt hetkeolukorrale siseministeeriumile. PVTK sõjalist luuretegevust välisriikide vastu Soome seadusandlus ei reguleeri. Seda tegevust juhitakse asutusesiseste korralduste ja Kaitsejõudude suunistega.

Ühendkuningriigi regulatsiooni ülevaates kirjeldati Julgeolekuteenistuse (Security Service (MI5)), Salaluureteenistuse (Secret Intelligence Service (MI6)) ning Valitsusside Peakorteri (Government Communications Headquarters (GCHQ)) tegevuse õiguslikku raamistikku. Ühendkuningriigi julgeoleku- ja luureasutuste tegevust reguleerivaid õigusakte ei ole palju. Samas reguleerivad julgeoleku- ja luureasutuste tegevust lisaks õigusaktidele tegevusjuhised, mille eesmärk on anda julgeoleku- ja luureasutustele praktilisi juhiseid, kas ja millistel tingimustel võib seaduses sätestatud meetmeid kasutada ning mis protseduure tuleb meetmete kasutamisel järgida.

Hollandi regulatsiooni ülevaates kirjeldati üldise luure- ja julgeolekuteenistuse (De Algemene Inlichtingen-en Veiligheidsdienst (AIVD)) ja Kaitseväe luure- ja julgeolekuteenistuse (Militaire Inlichtingen-en Veiligheidsdienst (MIVD)) tegevuse õiguslikku raamistikku. Hollandi julgeoleku- ja luureasutuste regulatsioon on süstematiseeritud ning koondunud ühte luure- ja julgeolekuseadusesse, mida täiendab julgeolekukontrolli seadus.

Saksamaa regulatsiooni ülevaates kirjeldati Riikliku Konstitutsioonikaitse Ameti (Bundesamt für Verfassungsschutz – BfV), Militaarse Vastuluure (Der Militärischen Abschirmdienst - MAD) ning Riikliku Luureteenistuse (Bundesnachrichtendienst – BND) tegevuse õiguslikku raamistikku. Saksamaa julgeoleku- ja luureasutuste tegevuse regulatsiooni iseloomustab hea organiseeritus. Iga julgeolekuasutuse tegevust reguleerib eraldi seadus. Samas võib regulatsioonidele ette heita ebaselgust. Näiteks ei ole piisavalt selgelt sõnastatud, millistel juhtudel julgeolekuasutused vastavaid meetmeid kasutada võivad ning milline täpsemalt on nende meetmete ulatus ja sisu.

Võrdleva analüüsi tulemusena selgus, et uuringus käsitletud riikide julgeoleku- ja luureasutuste volitustes ja meetmetes ei ole võrreldes Eestiga väga suuri erinevusi. Peamised erinevused tulenevad sellest, milliseid funktsioone julgeoleku- ja luureasutused täidavad. Eestis on näiteks Kaitsepolitseiametil nii vastuluure, korrakaitse kui ka süüteomenetluse funktsioonid, mistõttu täidab Kaitsepolitseiamet ka politsei ülesandeid. Eestiga sarnaselt täidavad politsei ülesandeid Soomes SUPO ning Rootsis SÄPO. Hollandis, Saksamaal ja Ühendkuningriigis on seevastu julgeoleku- ja luureasutused selgelt politseiasutustest eraldatud ning need asutused ei tegele kuritegude uurimisega. Seetõttu ei näe Hollandi, Saksamaa ja Ühendkuningriigi õigus ette selliseid meetmeid nagu isiku vahistamine, sõiduki peatamine, liikumisvabaduse piiramine jne.

Võrreldes Eesti julgeoleku- ja luureasutustega on Ühendkuningriigi julgeoleku- ja luureasutustel oluliselt ulatuslikumad volitused ja meetmed, sest Ühendkuningriigi regulatsioon näeb ette õiguse koguda massiliselt andmeid, sh elektroonilise side andmeid. Samuti pole võrreldes teiste riikidega Eesti õiguses selgelt reguleeritud krüpteeritud andmete uurimist, nagu see on reguleeritud Rootsis, Hollandis ja Ühendkuningriigis. Samuti puuduvad Eesti õiguses meetmetena näiliste tehingute tegemine (Soome) ning kontrollitud ligipääsu lubamine (Soome). Sarnaselt Eestiga on väljaspool riigi territooriumi lubatud tegutseda Ühendkuningriigi, Hollandi ning Saksamaa konkreetsetel julgeoleku- ja luureasutustel. Rootsi ja Soome õigus sellist võimalust ette ei näe.

Julgeolekukontrolli teostamisel on julgeoleku- ja luureasutustel Eesti õiguse kohaselt võimalik kasutada erinevaid julgeolekuasutuste seaduses sätestatud jälitustoiminguid. Seega annab Eesti õigus väga laiaulatuslikud volitused võrreldes teiste riikidega, eelkõige Soome, Rootsi, Saksamaa ning Hollandiga, kus julgeoleku- ja luureasutustel ei ole julgeolekukontrolliks jälitustoiminguid lubatud kasutada.

Võrreldes riigisiseste meetmete jagunemist asutuste vahel, siis Eestis, Soomes ja Rootsis on igal julgeoleku- ja luureasutusel omad meetmed vastavalt oma ülesannetele. Hollandi, Saksamaa ja Ühendkuningriigi julgeoleku- ja luureasutustel on aga kõigil riigisiseselt samad meetmed (mõningate eranditega).

Põhiõiguste riive õiguspärasuse tagamise protseduuride analüüsist nähtus, et kõikides riikides tuleb meetmete valimisel ja rakendamisel lähtuda põhiõiguste kaitse ja proportsionaalsuse põhimõttest. Võrreldes Eesti regulatsiooniga seisneb erinevus teiste riikide puhul detailsuse astmes. Näiteks Ühendkuningriigi regulatsioon sätestab iga meetme puhul eraldi, millistel tingimustel on meetme kasutamine vajalik. Soome õigus loetleb iga meetme puhul eraldi, milliste kuritegude tõkestamiseks või uurimiseks ning millistel tingimustel meetme kasutamine lubatud on.

Põhiõiguste riive õiguspärasuse tagamise protseduurid erinevad muus osas aga oluliselt. Eesti regulatsioon näeb ette eelneva kohtulikku kontrolli sõnumi saladust rikkuva või väga tõsise kodu, perekonna- või eraelu puutumatuse rikkumise korral (varjatud sisenemine ruumi, hoonesse, arvutisüsteemi jne). Samas toimub enamuse meetmete kasutamine siiski kas prokuratuuri või asutuse juhi loal ning mitmete meetmete kasutamiseks puudub üldse loamehhanism (nt teatud juhtudel elektroonilise side meta-andmete küsimisel). Rootsis seevastu peab reeglina meetme kasutamiseks taotlema kohtult luba. Ka Soome õigus näeb ette enamuse meetmete puhul eelneva kohtuliku kontrolli, mille kõrval on osasid meetmeid lubatud rakendada ameti juhi loal või ametniku enda otsuse alusel. Hollandi õigus näeb ette kohtult loa küsimise üksnes postisaadetiste avamiseks. Ühendkuningriigi õigus

kohtult loa taotlemist ette ei näe. Hollandis, Saksamaal ja Ühendkuningriigis on enamuse meetmete rakendamiseks vajalik ministri luba (teatud juhtudel ka asutuse juhi või kohtu luba).

Sellist rolli meetmete rakendamise üle otsustamisel nagu on prokuratuuril Eestis, teistes riikides ei ole. Rootsis võib teatud meetmeteks erand juhtudel loa anda ka prokurör, kui kohtu loa saamine tooks kaasa viivituse, mis takistab kuriteo ärahoidmist või takistab oluliselt uurimist. Samuti näeb Rootsi ja Soome regulatsioon erinevalt Eesti õigusest ette juristi või riikliku esindaja osalemise osade meetmete loamenetluses, kaitsmaks üksikisiku õiguseid.

Üldjoontes näevad Eesti, Soome, Rootsi, Hollandi ja Saksamaa regulatsioonid ette isiku teavitamise tema suhtes kasutusele võetud meetmetest. Teavitamise kord on riigiti erinev, sõltudes sealhulgas sellest, millise meetmega on tegemist. Samas on kõigis neis riikides võimalik teavitamist edasi lükata, kui esinevad teatud kaalukad põhjused (nt ohustab uurimist). Teavitamise kohustust ei näe ainsana ette Ühendkuningriigi regulatsioon.

Nagu põhiõiguste riive õiguspärasuse tagamise protseduuride puhul, erinevad ka järelevalvemehhanismid (*ex post*) oluliselt üksteisest. Eesti regulatsioon näeb ette teenistusliku järelevalve, Kaitsepolitseiameti puhul teatud juhtudel prokuratuuri järelevalve, parlamendi komisjoni järelevalve ning õiguskantsleri järelevalve. Ühine sarnane joon kõigi riikide puhul on see, et julgeoleku- ja luureasutuste üle teostab järelevalvet parlamentaarne komisjon. Sarnaselt Eestiga, on sätestatud selge teenistuslik järelevalve üksnes Soomes, Hollandis ning Ühendkuningriigis. Õiguskantsleri või ombudsmani järelevalvet ei ole kehtestatud samas Saksamaal ega Ühendkuningriigis.

Rootsi ja Ühendkuningriigi regulatsioonid näevad erinevalt Eesti regulatsioonist ette spetsialiseerunud asutused või institutsioonid, kes tegelevad just julgeoleku- ja luureasutuste järelevalvega. Näiteks Rootsis tegelevad Julgeoleku ja Isikuandmete Kaitse Komisjon ning Riiklik Kaitseteabe Inspektsioon üksnes julgeoleku- ja luureasutuste suhtes esitatud kaebustega, mille raames kontrollitakse, kas isikut puudutavaid andmeid on jälitustegevuse käigus kogutud ning kas kogumine on toimunud seadusega kooskõlas. Ühendkuningriigi üheks spetsialiseerunud institutsiooniks on luureasutuste erivolinik, kelle ülesandeks on kontrolli teostamine selle üle, kas julgeoleku- ja luureasutustele antud load on seaduslikud ning lubatud meetmeid on ka tegelikkuses teostatud seaduse kohaselt. Selleks on erivolinikul õigus valida välja ise konkreetsed juhtumid, käia asutustes jooksvalt kontrolle tegemas jne. Ühendkuningriigi uurimisvolituste tribunalil on õigus kohustada luure- või julgeolekuasutust tühistama loa, millega lubati meetme rakendamine, või kohustada luure- või julgeolekuasutust hävitama kogu informatsiooni, mis on loa alusel kogutud või mis on luure- või julgeolekuasutusel isiku kohta olemas. Erinevalt Eestist teevad Rootsi ja Saksamaa julgeoleku- ja luureasutuste üle järelevalvet ka andmekaitsega tegelevad asutused.

Elektroonilise side jälgimisel on nii Eestis kui ka teistes riikides lubatud jälgida nii elektroonilise side liiklusandmeid (meta-andmeid) kui ka elektroonilise side sisu. Erinevalt Eesti regulatsioonist näeb Ühendkuningriigi regulatsioon ette õiguse koguda ja säilitada massiliselt elektroonilise side andmeid. Samas on ka Rootsi puhul viidatud sarnasele ohule, et Raadioluureamet teostab elektroonilise side üldist jälgimist.

3. EESTI

3.1. Julgeoleku- ja luureasutused ning nende tegevust reguleerivad õigusaktid

Eestis on kaks julgeolekuasutust: **Kaitsepolitseiamet** ja **Teabeamet**. Lisaks nendele asutustele täidab luureülesandeid militaarvaldkonnas **Kaitsevägi**.

Kaitsepolitseiameti ja Teabeameti tegevust reguleerib julgeolekuasutuste seadus (JAS, RT I, 17.12.2015, 39), mis sätestab julgeolekuasutuste ülesanded, pädevuse ning suurema osa luure ja vastuluure meetmetest. JAS alusel on kehtestatud ka kaks ministri määrust, mis täpsustavad JAS sätestatud meetmeid ning vahendeid: 1) siseministri 06.06.2001 määrus nr 76 „Kaitsepolitseiameti poolt teabe varjatud kogumisel kasutatavad meetodid ja vahendid ning teabetoimiku pidamise ja säilitamise kord“ (RT I, 07.02.2013, 9); 2) kaitseministri 07.05.2001 määrus nr 37-TS-01 „Teabeameti poolt teabe varjatud kogumisel kasutatavad meetodid ja vahendid“ (RTL 2001, 58, 816).

Lisaks JASile reguleerivad julgeoleku- ja luureasutuste tegevust mitmed teised õigusaktid. Näiteks julgeoleku- ja luureasutuste tegevust riigisaladuse ja salastatud välisteabe kaitse valdkonnas reguleerib riigisaladuse ja salastatud välisteabe seadus (RSVS RT I, 12.03.2015, 46). Julgeolekukontrolli nn erisubjektide üle teostab Kaitsepolitseiamet kohtute seaduse (KS, RT I, 22.06.2016, 22), riigikontrolliseaduse (RKS, RT I, 30.12.2015, 70), õiguskantsleriseaduse (ÕKS, RT I, 06.04.2016, 23) ning Eesti Panga seaduse (EPS, RT I, 19.03.2015, 39) alusel. Tegutsemist väljaspool süüteomenetlust (nt teabehanke valdkonnas) reguleerib lisaks haldusmenetluse seadus (JAS § 1 lg 2).

Kaitsepolitseiametil on lisaks julgeoleku- ja luureülesannetele ka korrakaitselised (eelkõige kuritegude tõkestamine) ning süütegude menetlemise ülesanded. Kaitsepolitseiameti korrakaitseliste ülesannete hulka kuulub eriseadustes sätestatud riikliku järelevalve pädevus.

Korrakaitseliste ülesannete täitmisel reguleerivad Kaitsepolitsei tegevust seetõttu lisaks järgmised õigusaktid:

1) korrakaitseseadus (KorS, RT I, 23.03.2015, 207);
2) politsei ja piirivalve seadus (PPVS, RT I, 31.12.2015, 29);
3) kriminaalmenetluse seadustik (KrMS, RT I, 20.05.2016, 7);
4) Vabariigi Valitsuse 11.04.2016 määrus nr 60 „Politsei- ja Piirivalveameti ja Kaitsepolitseiameti vaheline uurimisalluvus“ (RT I, 07.04.2015, 5);
5) lennundusseadus (LennS, RT I, 03.05.2016, 7);
6) riigikaitseseadus (RiKS, RT I, 01.07.2016, 13);
7) isikut tõendavate dokumentide seadus (ITDS, RT I, 25.10.2016, 6);
8) välismaalaste seadus (VMS, RT I, 06.04.2016, 20);
9) välismaalasele rahvusvahelise kaitse andmise seadus (VRKS, RT I, 06.04.2016, 2);
10) strateegilise kauba seadus (StrKS, RT I, 12.03.2015, 48);
11) Euroopa Liidu kodaniku seadus (ELKS, RT I, 17.12.2015, 7);
12) väljasõidukohustuse ja sissesõidukeelu seadus (VSS, RT I, 06.04.2016, 22);
13) Eestit okupeerinud riikide julgeolekuorganite või relvajõudude luure- või vastuluureorganite teenistuses olnud või nendega koostööd teinud isikute arvelevõtmise ja avalikustamise korra seadus (OkuPS, RT I 1995, 17, 233).

Süütegude menetlemisel reguleerivad Kaitsepolitseiameti tegevust järgmised õigusaktid:

1) kriminaalmenetluse seadustik (KrMS, RT I, 20.05.2016, 7);
2) väärteomenetluse seadustik (VTMS, RT I, 19.03.2015, 37);
3) Vabariigi Valitsuse 11.04.2016 määrus nr 60 „Politsei- ja Piirivalveameti ja Kaitsepolitseiameti vaheline uurimisalluvus“ (RT I, 07.04.2015, 5);
4) elektroonilise side seadus (ESS, RT I, 17.05.2016, 2);
5) riigikaitseseadus (RiKS, RT I, 01.07.2016, 13);

6) strateegilise kauba seadus (StrKS, RT I, 12.03.2015, 48);
7) korruptsioonivastane seadus (KVS, RT I, 24.03.2016, 5).

Kaitseväeluure (militaarluure) toimub kaitseväe korralduse seaduse alusel (KKS, RT I, 06.07.2016, 8). Teabe kogumisel kasutatavad meetodid ja vahendid sätestab kaitseministri 01.09.2014 määrus nr 22 „Teabe kogumisel kasutatavad meetodid ja vahendid“ (RT I, 03.09.2014, 6).

Julgeolekuasutuste ligipääsu elektroonilise side andmetele reguleerib elektroonilise side seadus (ESS, RT I, 17.05.2016, 2), ligipääsu pangasaladusele krediidiasutuste seadus (KAS, RT I, 06.07.2016, 11). Järelevalvet julgeoleku- ja luureasutuste üle reguleerib lisaks muudele seadustele ka õiguskantsleri seadus (ÕKS, RT I, 06.04.2016, 23).

3.2. Julgeoleku- ja luureasutuste ülesanded, volitused ja meetmed põhiõiguste piiramisel

Julgeolekuasutuste tegevuse eesmärk on JAS kohaselt (§ 2 lg 1) tagada riigi julgeolek põhiseadusliku korra püsimisega mittesõjaliste ennetavate vahendite kasutamise abil ning julgeolekupoliitika kujundamiseks ja riigikaitseks vajaliku teabe kogumine ja töötlemine.

Teabeameti ülesanded on JAS § 7 alusel järgmised:

1) riigile välis-, majandus- ja riigikaitsepoliitika kujundamiseks ning riigikaitseks vajaliku välisriike, välismaiseid tegureid või tegevust puudutava teabe kogumine ja töötlemine (luure);
2) vastuluure teostamine riigi välisesinduste ja nende Kaitseväe struktuuriüksuste või nende teenistujate kaitseks, mis asuvad väljaspool riigi territooriumi;
3) vastuluure teostamine oma teenistujate, koostööle kaasatud isikute ja valduse kaitseks;
4) elektroonilise teabeturbe ning eriside korraldamine ja kontrollimine.

Lisaks eelnevale kuulub Teabeameti ülesannete hulka ametiabi andmine Kaitsepolitseiametile elektroonilisel viisil teabekogumisel (signaalluure, JAS § 7 lg 2) ning Kaitseväele kaitseväeluure teostamisel (JAS § 7 lg 2^1). Teabeamet tegeleb seega nii luure kui ka vastuluurega (vastuluure raames tegeleb ka julgeolekukontrolliga).

Kaitsepolitseiameti (KAPO) ülesanded on järgmised (JAS § 6):

1) riigi põhiseadusliku korra ja territoriaalse terviklikkuse vägivaldse muutmise ärahoidmine ja tõkestamine ning selleks vajaliku teabe kogumine ja töötlemine;
2) riigi vastu suunatud luuretegevuse ennetamine ja tõkestamine, sealhulgas riigisaladuse ja salastatud välisteabe kaitse riigisaladuse ja salastatud välisteabe seaduses ettenähtud juhtudel ja korras (v.a osas millega tegeleb Teabeamet) (vastuluure);
3) terrorismi ja selle rahastamise ning toetamise ärahoidmine ja tõkestamine ning selleks vajaliku teabe kogumine ja töötlemine;
4) riigi julgeolekut ohustava korruptsiooni ärahoidmine ja tõkestamine ning selleks vajaliku teabe kogumine ja töötlemine;
5) nende kuritegude tõkestamine, mille kohtueelne uurimine on KAPO pädevuses, (v.a osas, mis kuulub Teabeameti vastuluure pädevusse);
6) seadusega ettenähtud juhtudel kuritegude kohtueelne uurimine.

Vabariigi Valitsus kehtestab korraldusega iga aasta kohta riigi julgeolekuteabe hanke ja analüüsi kava. Selles sätestatakse julgeolekuasutustele ja Kaitseväele kaitseväeluure teostamisel esitatavad ülesanded ja kogutava teabe kava vastavalt selle olulisusele (JAS § 9 lg 2). Riigisaladuse ja salastatud välisteabe kaitseks teostab KAPO julgeolekukontrolli (RSVS § 48 lg 1)[3]. Samuti teostab KAPO taustakontrolli lennundusseaduse § 46^9 alusel. Kokkuvõttes täidab KAPO nii julgeoleku (vastuluure, eespool esitatud loetelu p 2), korrakaitse (st kuritegude tõkestamise, eespool esitatud loetelu punktid 1, 3–5) kui ka süüteomenetluse (eespool esitatud loetelu p 6) funktsioone. Kuigi JAS näeb ette kuritegude kohtueelse

[3] Samuti teostab KAPO julgeolekukontrolli nö erisubjektide (nt kohtunike) üle KS, RKS, ÕKS ja EPS alusel.

uurimise, on KAPO-l väärteomenetluses kohtuvälise menetleja pädevus KarS § 277 lõigetes 1 ja 1[1] ettenähtud väärtegude[4] puhul (VTMS § 52 lg 7), samuti ESS § 188 lg 5[5], RiKS § 96 lg 5 p 1[6], StrKS § 95 lg 2[7] ning KVS § 21 lg 2[8] alusel.

Põhiseadusliku korra kaitse eesmärgil täidab luureülesandeid lisaks Teabeametile ka **Kaitsevägi** (JAS § 2 lg 2). Kaitseväeluureks loetakse teabe kogumist ja töötlemist Kaitseväe poolt (KKS § 36 lg 1):

1) riigi sõjaliseks kaitsmiseks;
2) rahvusvahelise sõjalise operatsiooni ettevalmistamiseks ja läbiviimiseks;
3) riigi vastu suunatud luuretegevuse ennetamiseks või tõkestamiseks riigisaladuse ja salastatud välisteabe seaduses ettenähtud juhtudel ja korras (vastuluure);
4) rahvusvahelise sõjalise operatsiooni piirkonnas operatsioonil osaleva Kaitseväe üksuse kaitseks KKS ettenähtud korras;
5) taustakontrolli teostamiseks.

Kaitseväe struktuuriüksusena tegutseb luurekeskus, mille ülesandeks on (KKS § 22[3]):

1) teostada kaitseväeluuret ja koordineerida teiste struktuuriüksuste luure- ja julgeolekutegevust;
2) anda valdkonna eest vastutavale ministrile, Kaitseväe juhatajale ja Kaitseväe juhataja asetäitjale luure- ja julgeolekuteavet;
3) muude õigusaktidest tulenevate ülesannete täitmine.

Seega teostab Kaitsevägi nii luure kui ka vastuluure ülesandeid.

3.2.1. Teabeameti volitused ja meetmed

Teabeameti volitused ja meetmed[9] on sätestatud JAS 4. peatükis. JAS alusel on Teabeametil volitus koguda ja töödelda teavet, sh isikuandmeid, kui see on vajalik Teabeameti ülesannete täitmiseks (§ 3 lg 1). Andemete kogumiseks on Teabeametil sealjuures pädevus piirata isiku õigust sõnumi saladusele (JAS § 25) ning piirata isiku õigust kodu, perekonna- või eraelu puutumatusele (JAS § 26). Otsese ohu korral riigi julgeolekule, on Teabeametil õigus nõuda oma ülesannete täitmiseks vastava abi osutamist üksikisikult (JAS § 22 lg 2).

Teabeamet teostab vastuluuret nii väljaspool Eesti Vabariiki (riigi välisesinduste kaitseks) kui ka Eesti Vabariigi territooriumil. Eesti territooriumil võib Teabeamet vastuluuret teostada üksnes oma teenistujate, koostööle kaasatud isikute ja valduse kaitseks (JAS § 7 lg 1 p 3).

Kuivõrd Teabeameti põhiülesandeks on luure ja vastuluure teostamine julgeoleku tagamiseks, ei ole Teabeameti esmaseks ülesandeks kuritegude avastamine ja tõkestamine selle tavalises tähenduses (nagu KAPO puhul), vaid Eesti Vabariigi, Eesti kodanike ning teiste riikide ja isikute julgeoleku tagamine.[10] Samas võib laiemas plaanis meetmeid julgeoleku tagamiseks käsitleda kavandatava (üldjuhul KarS järgi

[4] Ametniku vormiriietuse ja ametitunnistuse ebaseaduslik kasutamine.
[5] Jälitus- ja julgeolekuasutusele teabe andmise ning sidevõrgule juurdepääsu võimaldamise kohustuse rikkumine, Jälitustoimingu teostamise ja eraelu puutumatuse õiguse piiramise ning sõnumi saladuse õiguse piiramise toimingu andmete saladuses hoidmise kohustuse rikkumine.
[6] Riigikaitseobjekti füüsilise kaitse nõuete rikkumine.
[7] Teavitamiskohustuse, strateegilise kauba eriloa tingimuste, dokumentide säilitamise ja aruandekohustuste eiramine.
[8] Ametiseisundi, avaliku vahendi, mõju või siseteabe korruptiivne kasutamine, korruptiivse tulu saamisega seotud teatamise ja üleandmise kohustuse rikkumine, toimingupiirangu rikkumine.
[9] Seaduse tasemel ei eristata, millised sätted käsitlevad julgeolekuasutuste volitusi ning millised meetmed. Seaduse mõttest on siiski aru saada, et volituste all mõeldakse pädevust koguda ja töödelda andmeid, piirata selleks isikute sõnumisaladust ning kodu, perekonna- või eraelu puutumatust. Meetmed on seevastu konkreetsed abinõud, kuidas andmeid kogutakse või kuidas sõnumisaladusse sekkutakse.
[10] Ü. Madise jt (toim). Eesti Vabariigi põhiseadus. Komm vlj. 3. vlj. Tallinn: Juura 2012. § 43/13.1.

riigivastase) kuriteo tõkestamisena.[11] Sellest võib järeldada, et JAS-s sätestatud meetmeid, mille kasutamine on ettenähtud üksnes kuritegude tõkestamiseks, on lubatud kasutada ka luure ja vastuluure ülesannete täitmisel. Näiteks võib eelneva põhjal järeldada, et JAS § 25 sätestatud volitus piirata isiku õigust sõnumisaladusele on antud ka Teabeametile, kuigi JAS § 25 lg 2 sõnastuse kohaselt võib julgeolekuasutus oma pädevuse piires piirata isiku õigust sõnumi saladusele kuriteo tõkestamiseks, kui on olemas piisavad andmed ettevalmistatava või toimepandava kuriteo kohta. Eelnevat tõlgendust kinnitab asjaolu, et ametiabi korras võib Kaitseväe juhataja taotleda Teabeametilt riigi sõjaliseks kaitsmiseks vajaliku teabe kogumist JAS §-s 25 kirjeldatud viisil sõnumite saladust riivates (KKS § 39). Seega võib järeldada, et Teabeametil on kõik JAS-s sätestatud volitused ning õigused kasutada meetmeid, mis ei ole konkreetselt antud KAPO-le.

Seetõttu võib Teabeamet luure ja vastuluure eesmärgil kasutada järgmiseid meetmeid:

1) riigiasutuselt, avalik-õiguslikult asutuselt, füüsiliselt isikult abi nõudmine (JAS § 22);
2) isiku, asutuse ja organi teesklemine (JAS § 23);
3) postisaadetise läbivaatus (JAS § 25 lg 3 p 1);
4) elektroonilise side võrgu kaudu edastatava sõnumi või muu teabe pealtkuulamine, -vaatamine või salvestamine (JAS § 25 lg 3 p 2);
5) muul viisil edastatava teabe pealtkuulamine, -vaatamine või salvestamine (JAS § 25 lg 3 p 3).
6) kuriteo tõkestamiseks sisenemine isiku ruumi, hoonesse, piirdega alale, sõidukisse või arvutisüsteemi ilma isiku nõusolekuta ja nende läbiotsimine (JAS § 26 lg 2);
7) isikuandmete kogumine (JAS § 26 lg 3 p 1);
8) varjatud jälgimine (JAS § 26 lg 3 p 2);
9) isiku samasuse varjatud tuvastamine (JAS § 26 lg 3 p 3);
10) elektroonilise side võrgu kaudu edastatavate sõnumite edastamise fakti, kestuse, viisi ja vormi ning edastaja või vastuvõtja isikuandmete ja asukoha kohta andmete kogumine (JAS § 26 lg 3 p 4);
11) varjatult sisenemine ruumi, hoonesse, piirdega alale, sõidukisse või arvutisüsteemi teabe varjatud kogumiseks, salvestamiseks või selleks vajalike tehniliste abivahendite paigaldamiseks ja eemaldamiseks (JAS § 26 lg 3 p 5);
12) asja varjatult läbivaatamine ning vajaduse korral selle varjatult muutmine, rikkumine või asendamine (JAS § 26 lg 3 p 6);
13) riigi- või kohaliku omavalitsuse asutuselt või avalik-õiguslikult juriidiliselt isikult andmete saamine (JAS § 31 lg 1);
14) füüsiliselt või eraõiguslikult juriidiliselt isikult vajaliku teabe saamine (JAS § 31 lg 2);
15) juurdepääs avaliku teabe seaduse alusel asutatud andmekogu andmetele (JAS § 31^1);
16) õigus kanda tulirelva ning kasutada seda äärmise abinõuna (JAS § 35).

Teabe varjatud kogumisel kasutatavaid meetmeid ja vahendeid täpsustab JAS § 28 alusel kehtestatud kaitseministri 07.05.2001 määrus nr 37-TS-01 „Teabeameti poolt teabe varjatud kogumisel kasutatavad meetodid ja vahendid“. Kuivõrd see määrus on salastatud, ei käsitle käesolev analüüs selles sätestatud meetodeid ja vahendeid.

Teabeamet teostab vastuluure raames julgeolekukontrolli (RSVS § 48 lg 3). RSVS § 49 lg 1 kohaselt teostatakse julgeolekukontrolli julgeolekuasutuste seaduses sätestatud korras, arvestades RSVS-s sätestatud erisustega. Kuivõrd JAS-s ei ole julgeolekukontrolli teostamise korda kui sellist sätestatud, siis on julgeolekukontrolliks võimalik kasutada kõiki vastuluure meetmeid. Seega on julgeolekukontrollis lubatud kasutada kõiki JAS 4. peatükis sätestatud sõnumisaladuse, eraelu ja perekonna ning kodu puutumatuse kaitset riivavaid vastuluure meetmeid (vt eespool).

JAS-is sätestatud ülesannete täitmiseks, samuti julgeolekukontrolli teostamiseks on Teabeametil juurdepääs pangasaladusele (KAS § 88 lg 5 p 3).

[11] Ü. Madise jt (toim). Eesti Vabariigi põhiseadus. Komm vlj. 3. vlj. Tallinn: Juura 2012. § 43/13.1.

3.2.2. Kaitsepolitseiameti volitused ja meetmed

KAPO volitused ja meetmed[12] on sätestatud nii JAS-s kui ka teistes seadustes (PPVS, KorS, KrMS) vastavalt sellele, milliseid ülesandeid KAPO täidab.

JAS alusel on KAPO-l volitus koguda ja töödelda teavet, sh isikuandmeid, kui see on vajalik julgeolekuasutuse ülesannete täitmiseks (§ 3 lg 1). Andmete kogumiseks on KAPO-l sealjuures pädevus piirata isiku õigust sõnumi saladusele (JAS § 25) ning piirata isiku õigust kodu, perekonna- või eraelu puutumatusele (JAS § 26). Otsese ohu korral riigi julgeolekule on julgeolekuasutusel õigus nõuda oma ülesannete täitmiseks vastava abi osutamist üksikisikult (JAS § 22 lg 2).

Kuna KAPO tegeleb ka korrakaitseliste ülesannetega, on lisaks eelnevale KAPO-l[13] volitus kohaldada riiklikku järelevalve meetmeid (korrakaitseseaduses sätestatud alustel ja korras), vahetut sundi (JAS § 21 lg 2) ning teostada KrMS-s sätestatud jälitustoiminguid.

Julgeoleku- ja luureasutuste regulatsioonile on varasemalt ette heidetud seda, et JASis ja teistes seadustes ei ole piisavalt selgelt määratletud, milliste ülesannete täitmiseks, millised volitused ja meetmed KAPO-l on.[14] Näiteks JAS § 26 lg 2 alusel võib julgeolekuasutus kuriteo tõkestamiseks ja julgeoleku tagamise eesmärgil siseneda isiku ruumi, hoonesse, piirdega alale, sõidukisse või arvutisüsteemi ilma isiku nõusolekuta ja neid läbi otsida. Ebaselgeks jääb samas, milliste ülesannete täitmiseks (kas ja millistel alustel) on lubatud riived kodu, perekonna- ja eraelu puutumatusele JAS § 26 lg 3-s sätestatud meetmetega (varjatud jälgimine, isiku samasuse varjatud tuvastamine, asja varjatud läbivaatamine jne).

Samuti on leitud, et mõningail juhtudel võib samal eesmärgil tehtavaid toiminguid teha erinevatel õiguslikel alustel, nt ettevalmistatava kuriteo tõkestamine on võimalik nii KrMS § 126^2 lg 1 p 1 kui ka JAS normide alusel.[15] Samas on ka teistsuguseid arvamusi, milles leitakse, et JAS-s sätestatud meetmete rakendamise pädevus piirneb üksnes vastuluure menetluse teabehankeliste raamidega ega laiene KAPO ennetavale tegevusele (korrakaitselistele ülesannetele).[16] Selline tõlgendus läheks aga vastuollu JAS kehtiva sõnastusega, näiteks eelnimetatud JAS § 26 lg-ga 2, mille alusel võib kuriteo tõkestamiseks siseneda ruumi ilma isiku loata.

Lisaks on mõneti ebaselge PPVSi kohaldumine KAPO tegevusele. Kuigi JAS § 21 lõikest 1 ei selgu otseselt, milliste tegevuste (kas vastuluure, korrakaitse või süütegude menetlemise) jaoks PPVS-s sätestatud meetmeid kohaldada võib, on õigus PPVS meetmeid kasutada nii vastuluures kui ka korrakaitseliste ülesannete täitmiseks[17]. Kriminaalmenetlusele PPVS-s sätestatud meetmed ei kohaldu, sest PPVS § 1 lg 4 alusel on politsei ülesanded ja tegevus süüteomenetluses sätestatud kriminaalmenetluse seadustikus ja väärteomenetluse seadustikus. Ehk teisisõnu on süütegude menetlemiseks kehtestatud selge eriregulatsioon. Samuti, kuivõrd kriminaalmenetluse seadustik on

---

[12] Seaduse tasemel ei eristata, millised sätted käsitlevad julgeolekuasutuste volitusi ning millised meetmeid. Seaduse mõttest on siiski aru saada, et volituste all mõeldakse pädevust koguda ja töödelda andmeid, rikkuda selleks isikute sõnumisaladust ning kodu, perekonna- või eraelu puutumatust. Meetmed on seevastu konkreetsed abinõud, kuidas andmeid kogutakse või kuidas sõnumisaladusse sekkutakse.

[13] JAS § 21 lg 2 annab selle volituse üksnes KAPO teenistuses olevatele politseiametnikele, mitte kõigile KAPO ametnikele.

[14] Õiguskantsler. (2015). Arvamus julgeolekuasutuste seaduse ning politsei ja piirivalve seaduse muutmise seaduse eelnõu väljatöötamise kavatsusele. Kättesaadav aadressilt http://oiguskantsler.ee/sites/default/files/field_document2/6iguskantsleri_arvamus__julgeolekuasutuste_seaduse_ning_politsei_ja_piirivalve_seaduse_muutmise_seaduse_eelnou_valjatootamise_kavatsus.pdf

[15] Õiguskantsler. (2015). Arvamus julgeolekuasutuste seaduse ning politsei ja piirivalve seaduse muutmise seaduse eelnõu väljatöötamise kavatsusele. Kättesaadav aadressilt http://oiguskantsler.ee/sites/default/files/field_document2/6iguskantsleri_arvamus__julgeolekuasutuste_seaduse_ning_politsei_ja_piirivalve_seaduse_muutmise_seaduse_eelnou_valjatootamise_kavatsus.pdf

[16] A. Lott. Põhiseadusliku korra kaitseks teostatav jälitustegevus Eestis. Riigikohus: Tartu 2015. – http://www.riigikohus.ee/vfs/1906/PKK%20j%E4litustegevuse%20anal%FC%FCs.pdf , lk 10.

[17] vt ka A. Lott. Põhiseadusliku korra kaitseks teostatav jälitustegevus Eestis. Riigikohus: Tartu 2015, lk 10

konstitutsiooniline seadus, ei saa reguleerida KAPO tegevust kriminaalmenetluses muu seadusega, mis ei ole võetud vastu Riigikogu koosseisu enamuse poolt. Seega võib järeldada, et PPVS-s sätestatud meetmeid võib kasutada nii vastuluure kui ka korrakaitseliste ülesannete täitmiseks, kuid mitte süütegude menetlemiseks.

Kuivõrd KAPO täidab erinevaid funktsioone, millest tulenevalt on KAPO-l ka erinevad volitused ja meetmed, käsitletakse meetmeid järgmistes gruppides: 1) vastuluures kasutatavad meetmed; 2) korrakaitseks kasutatavad meetmed; 3) süütegude menetlemiseks kasutatavad meetmed.

(a) Vastuluures kasutatavad meetmed

KAPO võib vastuluure eesmärgil (teabehankeks) ehk JAS § 6 punktis 2 sätestatud ülesande täitmiseks kasutada nii JAS-s kui ka PPVS-s sätestatud meetmeid. Kuivõrd JAS alusel sätestatud meetmed on sisuliselt samad, mis Teabeametil, mida käsitleti alapeatükis 1.2.1., käsitletakse käesolevas osas üksnes JAS alusel kehtestatud siseministri määruses[18], PPVS-s ja RSVS-s sätestatud meetmed.

Siseministri määruse[19] alusel kasutab KAPO järgmiseid meetmeid:

1) postisaadetiste vahetu läbivaatus avamise, läbivalgustamise ja sulgemise teel ning saadud informatsiooni talletamine, kasutades vastavaid tehnilisi vahendeid või vastavalt kohaldatud tehnoloogiaid (§ 1 lg 1 p 1);
2) telegraafi, telefoni või muu tehnilise sidekanali[20] kaudu edastatava sõnumi või muu teabe pealtkuulamine, -vaatamine või salvestamine, kasutades vastavaid tehnilisi vahendeid või vastavalt kohaldatud tehnoloogiaid (§ 1 lg 1 p 2);
3) muul viisil edastatava teabe[21] pealtkuulamist, -vaatamist või salvestamist, paigaldades selleks vajalikke tehnilisi vahendeid (§ 1 lg 1 p 3);
4) isikuandmete kogumine riigi, kohalike omavalitsuste, avalik-õiguslike või eraõiguslike isikute või asutusesisestest andmekogudest ning sealhulgas andmekogude ristkasutamine ja arhiivimaterjalide kogumine (§ 2 p 1);
5) varjatud jälgimine visuaalselt või jälgimisseadmete[22] abil (§ 2 p 2);
6) isiku samasuse varjatud tuvastamine riigi, kohalike omavalitsuste, avalik-õiguslike või eraõiguslike isikute andmekogude ristkasutamise või arhiivimaterjalide kogumise teel (§ 2 p 3);
7) telekommunikatsioonivõrgu kaudu edastatavate sõnumite edastamise fakti, kestuse ja viisi ning edastaja või vastuvõtja kohta andmete kogumine päringuga telekommunikatsioonivõrgu operaatorile või telekommunikatsiooniteenuse osutajale (§ 2 p 4);
8) varjatud sisenemine eluruumi, muusse ehitisse või valdusse, andmekogusse, töökohta või sõidukisse teabe varjatud kogumiseks või salvestamiseks või selleks vajalike abivahendite paigaldamist, kasutades vastavaid tehnilisi vahendeid või vastavalt kohaldatud tehnoloogiaid ja võtteid (§ 2 p 5);
9) isiku kaasamine salajasele koostööle (§ 3).

Punktides 1–8 nimetatud meetmete rakendamiseks kasutab KAPO omakorda täiesti salajasi meetodeid ja vahendeid (§ 1 lg 1 ja § 2).Võrreldes JAS-ga sätestab siseministri määrus seega ühe täiendava meetme – isiku kaasamine salajasele koostööle.

---

[18] Siseministri 06.06.2001 määrus nr 76 „Kaitsepolitseiameti poolt teabe varjatud kogumisel kasutatavad meetodid ja vahendid ning teabetoimiku pidamise ja säilitamise kord“ (RT I, 07.02.2013, 9).
[19] Siseministri 06.06.2001 määrus nr 76 „Kaitsepolitseiameti poolt teabe varjatud kogumisel kasutatavad meetodid ja vahendid ning teabetoimiku pidamise ja säilitamise kord“ (RT I, 07.02.2013, 9).
[20] Telegraafi, telefoni või muu tehnilise sidekanali kaudu edastatava sõnumi või muu teabe pealtkuulamine, -vaatamine või salvestamine hõlmab kõiki audio-video, telekommunikatsioonivõrgu signaalide või kosmoseside edastamise liike.
[21] See hõlmab isikute poolt ja vahendusel edastatavat teavet, signaale ja andmeid.
[22] Jälgimisseadena käsitletakse tehnilisi vahendeid, mis võimaldavad jälgida ja jälitada isikuid, nende vara ning muid objekte

Lisaks JAS-s sätestatud meetmetele on KAPO-l vastuluures volitus kasutada ka **PPVS-s** sätestatud meetmeid (JAS § 21 lg 1). Need meetmed on:

1) päringu tegemine sideettevõtjale (elektroonilise side võrgu kaudu edastatavate sõnumite edastamise fakti, kestuse, viisi ja vormi ning edastaja või vastuvõtja isikuandmete ja asukoha kohta andmete kogumiseks) (PPVS § 7^{49});
2) isiku kaasamine salajasele koostööle[23] (PPVS § 7^{51});
3) konspiratsioonivõtete kasutamine[24] (PPVS § 7^{54});
4) teesklemine[25] (PPVS § 7^{55});
5) variisiku[26] kasutamine (PPVS § 7^{56}).

KAPO teostab **RSVS** alusel vastuluures ka julgeolekukontrolli (RSVS § 48 lg 1). RSVS § 49 lg 1 kohaselt teostatakse julgeolekukontrolli julgeolekuasutuste seaduses sätestatud korras, arvestades RSVS-s sätestatud erisustega. Kuivõrd JAS-s ei ole julgeolekukontrolli teostamise korda kui sellist sätestatud, siis on julgeolekukontrolliks võimalik kasutada kõiki vastuluure meetmeid. Seega on julgeolekukontrollis lubatud kasutada kõiki JAS 4. peatükis sätestatud sõnumisaladuse, eraelu ja perekonna ning kodu puutumatuse kaitset riivavaid vastuluure meetmeid (RSVS § 49 lg 1). KS (§ 54 lg 4), RKS (§ 18 lg 3), ÕKS (§ 6^1 lg 3) ja EPS (§-d 11^1 lg 3, § 11^2 lg 3) alusel julgeolekukontrolli teostamisel nn erisubjektide üle, lähtub KAPO JAS-st (seega on võimalik kasutada kõiki vastuluure meetmeid).

JAS-is sätestatud ülesannete täitmiseks, samuti julgeolekukontrolli teostamiseks on KAPO-l juurdepääs pangasaladusele (KAS § 88 lg 5 p 3).

(b) Korrakaitseks kasutatavad meetmed

KAPO volitused ja meetmed kuritegude ettevalmistamise avastamisel ja tõkestamisel ehk JAS § 6 punktides 1, 2^1 – 3 sätestatud ülesannete täitmiseks tulenevad JAS-st, KrMS-st, KorS-ist ja PPVS-st. Riikliku järelevalve teostamiseks eriseaduste alusel (nt LennS, StrKS, ELKS jne) antakse vastava eriseadusega õigus kohaldada KorS-i erimeetmeid ja vahetut sundi. JAS-s sätestatud meetmeid kirjeldati alapeatükis 1.2.1., samuti kirjeldati eelmises alapunktis (*Vastuluures kasutatavad meetmed*) nii siseministri 06.06.2001 määruses nr 76 kui PPVS-s sätestatud meetmeid.

Kriminaalmenetluse seadustiku mõttes on KAPO korrakaitselisi ülesandeid täites käsitatav jälitusasutusena (§ 126^2 lg 1) ja uurimisasutusena (KrMS § 31 lg 1). KAPO võib jälitusasutusena teha jälitustoimingu[27] teabe kogumiseks kuriteo ettevalmistamise kohta selle avastamise või tõkestamise eesmärgil (KrMS § 126^2 lg 1 p 1 ja lg 5). Selle eelduseks on, et kuritegu on KAPO uurimisalluvuses, mis on määratud Vabariigi Valitsuse 11.04.2016 määrusega nr 60 „Politsei- ja Piirivalveameti ja Kaitsepolitseiameti vaheline uurimisalluvus“[28] ning et tegemist on KrMS § 126^2 lg 2 loetletud kuriteoga.

KrMS alusel võib KAPO kuriteo ettevalmistamise avastamise ja tõkestamise eesmärgil teostada järgmiseid jälitustoiminguid:

1) jälgida varjatult isikut, asja või paikkonda (KrMS § 126^3 lg 1);
2) koguda varjatult võrdlusmaterjali ja teha esmauuringuid (KrMS § 126^3 lg 1);

[23] Salajasele koostööle kaasatud isik on isik, kelle koostöö politseiga ei ole kolmandatele isikutele teada.
[24] Mida konspiratsioonivõtte all täpsemalt mõeldakse, seda seadus ei täpsusta. Konspiratsioonivõtteid kasutatakse eesmärgiga varjata andmesubjekti eest jälitustoimingu tegijaid, jälitustoimingu eesmärki ning kasutatava kinnis- ja vallasasja kuuluvust.
[25] KAPO võib jälitustoimingu tagamiseks teeselda eraõiguslikku juriidilist isikut, tema struktuuriüksust või organit või välisriigi äriühingu filiaali.
[26] Variisik on isik, kes aitab tagada jälitustoimingu varjatust.
[27] Jälitustoiming on isikuandmete töötlemine seaduses sätestatud ülesande täitmiseks eesmärgiga varjata andmete töötlemise fakti ja sisu andmesubjekti eest (KrMS § 126^1 lg 1).
[28] KAPO uurimisalluvusse kuuluvad nt süüteod inimsuse ja rahu vastu, rahvusvahelise julgeoleku vastu, süüteod Eesti Vabariigi ja riigivõimu vasut (sh terrorismiga seotud kuriteod), riigi kaitsevõime vastu jne.

3) teostada varjatult asja läbivaatust ning asendada selle varjatult (KrMS § 126^3 lg 1);
4) vaadata varjatult läbi postisaadetist[29] (KrMS § 126^3 lg 2 p 1);
5) vaadata või kuulata salaja pealt teavet (KrMS § 126^3 lg 2 p 2);
6) kasutada politseiagenti[30] (KrMS § 126^3 lg 2 p 3).

Punktides 1 – 3 ja 5 – 6 nimetatud jälitustoimingu tegemisel on lubatud varjatult siseneda hoonesse, ruumi, sõidukisse, piirdega alale või arvutisüsteemi juhul, kui see on vältimatult vajalik jälitustoimingu eesmärgi saavutamiseks (KrMS § 126^3 lg 5).

KAPO-l on korrakaitseliste ülesannete täitmiseks lisaks õigus kohaldada **korrakaitseseaduses** sätestatud alustel ja korras riikliku järelevalve meedet ning vahetut sundi[31] (JAS § 21 lg 2). Riikliku järelevalve üldmeetmed on teavitamine (KorS § 26), ettekirjutuse ja haldussunnivahendi kohaldamine (KorS § 28) ning ohu tõrjumine või korrarikkumise kõrvaldamine (KorS § 29). KAPO-l on õigus kasutada ka mitmesuguseid riikliku järelevalve erimeetmeid:

1) küsitleda ja nõuda dokumente (KorS § 30);
2) kohaldada sundtoomist (KorS § 31);
3) tuvastada isiku samasus, sh eriliste tuvastusmeetmetega[32] (KorS §-d 32 ja 33);
4) kasutada avalikus kohas toimuva jälgimiseks pilti edastavat või salvestavat jälgimisseadmestikku (KorS § 34);
5) küsida sideettevõtjalt elektroonilise side meta-andmeid (KorS § 35);
6) saada juurdepääs mobiiltelefonivõrgus kasutatavate terminalseadmete asukoha tuvastamiseks reaalajas (KorS § 35);
7) töödelda hädaabinumbrile edastatud informatsiooni (KorS § 35^1);
8) kohaldada viibimiskeeldu (KorS § 44);
9) peatada sõidukeid (KorS § 45);
10) pidada isikut kinni kuni 48 h (KorS § 46);
11) teostada turvakontrolli (KorS § 47);
12) teostada isiku läbivaatust (KorS § 48);
13) teostada vallasasja läbivaatust, võtta see hoiule või müüa või hävitada (KorS §-d 49, 52, 53);
14) siseneda valdusesse ja vaadata see läbi (KorS §-d 50 ja 51).

Lennundusseaduse alusel teostab KAPO taustakontrolli isiku sobilikkuse hindamiseks lennuvälja või kopteriväljaku julgestuspiirangualale saatjata pääsemiseks, õhusõiduki meeskonnaliikme sertifikaadi või tunnistuse saamiseks ja lennundusjulgestusalaste ülesannete täitmiseks (LennS § 46^9). Milliseid meetmeid KAPO selleks rakendada võib, on seaduses sätestamata.

Samuti on korrakaitseliste ülesannete täimiseks KAPO-l juurdepääs pangasaladusele (KAS § 88 lg 5 p 3).

(c) Süütegude menetlemiseks kasutatavad meetmed

KAPO volitused ja meetmed süütegude menetlemisel (ehk JAS § 6 punktis 4 sätestatud ülesande täitmiseks) tulenevad KrMS-st.

Kriminaalmenetluse raames on KAPO käsitatav uurimisasutusena KrMS § 31 lg 1 mõttes ja jälitusasutusena KrMS § 126^2 lõike 1 mõttes. KrMS alusel võib KAPO teostada samu jälitustoiminguid,

[29] Postisaadetise varjatud läbivaatusel kogutakse saadetise kohta vaatlusandmeid ning pärast seda edastatakse saadetis adressaadile. Postisaadetise varjatud läbivaatuse käigus võib saadetise asendada.
[30] Politseiagent on isik, kes muudetud identiteeti kasutades kogub teavet.
[31] Vahetu sund on füüsilise isiku, looma või asja mõjutamine füüsilise jõuga, erivahendiga või relvaga (KorS § 74 lg 1).
[32] Nt daktüloskopeerimise või DNA-proovi võtmise vms.

mida kuriteo ettevalmistamise avastamise ja tõkestamise eesmärgilgi (vt eelmine punkt *Korrakaitseks kasutatavad meetmed*). Kriminaalmenetluse raames on aga lisaks võimalik matkida kuritegu (KrMS § 126^3 lg 3).

Lisaks jälitustoimingutele, võib KAPO teostada ka erinevaid menetlustoiminguid:

1) vaatlus (KrMS § 83);
2) isiku läbivaatus (KrMS § 88);
3) posti- või telegraafisaadetise arest ja läbivaatus (KrMS § 89);
4) andmete nõudmine sideettevõtjalt (KrMS § 90^1);
5) läbiotsimine (KrMS § 91);
6) uurimiseksperiment (KrMS § 93).

KAPO-l on volitus kasutada ka erinevaid kriminaalmenetluse tagamise vahendeid:

1) elukohast lahkumise keeld (KrMS § 128),
2) vahistamine (KrMS § 130),
3) rahatrahvi määramine (KrMS § 138^1),
4) sundtoomine (KrMS § 138^1),
5) tagaotsitavaks kuulutamine (KrMS § 140),
6) isiku samasuse tuvastamine (KrMS § 140^1),
7) viibimiskeeld (KrMS § 140^2),
8) kahtlustatava ja süüdistatava ametist kõrvaldamine (KrMS § 141),
9) vara arestimine (KrMS § 142).

Kriminaalmenetluse raames on KAPO-l juurdepääs pangasaladusele (KAS § 88 lg 5 p 2).

Väärteomenetluse raames on KAPO-l õigus nõuda füüsiliselt ja juriidiliselt isikult väärteoasja lahendamiseks vajaliku dokumendi, eseme või muu objekti esitamist (VTMS § 31 lg 2). Korruptsioonivääreteo puhul võib taotleda juurdepääsu pangasaladusele ja fondiosakute registri andmetele (VTMS § 31 lg 3). Samuti võib väärteomenetluse raames teha päringu sideettevõtjale elektroonilise side meta-andmete saamiseks (VTMS § 31^2). Jälitustoiminguid ei ole väärteomenetluse raames lubatud teha (VTMS § 32 lg 1). Väärteomenetluse raames võib isiku kinni pidada, kuid seda võib teha üksnes KAPO teenistusse kuuluv politseiametnik (VTMS § 44 lg 1, § 45 lg 1 p 1). Lisaks on KAPO-l õigus isiku läbivaatuse tegemiseks (VTMS § 34), läbiotsimiseks (VTMS § 35) ning kohaldada sundtoomist (VTMS § 43 lg 3).

3.2.3. Kaitseväe volitused ja meetmed

Kaitseväe volitused ja meetmed on kehtestatud KKS-s ning selle alusel kehtestatud kaitseministri määruses[33]. KKS alusel on kaitseväel volitus kaitseväeluure teostamiseks koguda ja töödelda:

1) väljaspool üldkasutatavat Eesti Vabariigi territooriumil asuvat elektroonilise side võrku edastatavaid või levivaid signaale;
2) pilte või kujutisi maa- või merepinna ja väljaspool Eesti Vabariigi territooriumi asuva või Eesti Vabariigi territooriumile sisenenud välisriigi kasutuses oleva objekti kohta;
3) muudelt teabevaldajatelt saadud juurdepääsupiiranguta teavet või avaliku teabe seaduses või riigisaladuse ja salastatud välisteabe seaduses sätestatud alustel saadud piiratud juurdepääsuga teavet;

[33] Kaitseministri 01.09.2014 määrus nr 22 „Teabe kogumisel kasutatavad meetodid ja vahendid“ (RT I, 03.09.2014, 6). See määrus on salastatud.

4) Teabeametilt saadud teavet, mis on kogutud isiku, asutuse või organi teesklemisega, sõnumisaladuse õiguse piiramise või kodu, perekonna- või – eraelu puutumatuse õiguse piiramisega, või
5) muul viisil avalikest allikatest saadud teavet (KKS § 37 lg 1).

Kaitseväel on õigus kaitseväeluure teostamiseks lisaks eelnevale:

1) rahvusvahelise sõjalise operatsiooni piirkonnas ja väljaspool Eesti Vabariigi territooriumi tegutsemiseks:
    a. isikuid küsitleda;
    b. isikuid varjatult jälgida;
    c. kaasata isikut salajasse koostöösse;
    d. teeselda eraõiguslikku juriidilist isikut, tema struktuuriüksust, organit või äriühingu filiaali;
    e. kasutada variisikut[34].
2) väljaspool Eesti Vabariigi territooriumi isikuid varjatult jälgida (KKS § 37 lg 2).

Väljaspool Eesti Vabariiki tegutsemiseks võib ettevalmistavaid tegevusi alustada juba Eesti Vabariigis. Isikute varjatud jälgimine saab toimuda aga üksnes väljaspool Eesti Vabariigi territooriumi, st Eesti Vabariigis ei ole kaitseväeluurel pädevust isikuid varjatult jälgida.[35]

Jälitusteabele juurdepääsu võimaldamise otsustamiseks või sõjaväepolitseis asuvale sõjaväelise auastmega ametikohale nimetamisel võib isiku kohta andmeid koguda:

1) KrMS §126[3] lõikes 1 nimetatud jälitustoimingutega: jälgida varjatult isikut, asja või paikkonda, koguda varjatult võrdlusmaterjali ja teha esmauuringuid, teostada varjatult asja läbivaatust ning asendada selle varjatult (KKS § 41[2] lg 1);
2) teha päring elektroonilise side meta-andmete kohta (KKS § 41[2] lg 1).

Kaitseväkke teenistusse või tööle kandideeriva isiku ning tegevväelase, ametniku või töötaja Kaitseväkke sobivuse hindamisel ja Kaitseväele teenuse osutamisega seotud isikute Kaitseväe julgeolekualale lubamise otsustamisel on Kaitseväel õigus läbi viia taustakontrolli (KKS § 41[3]). Kaitseväel on taustakontrolli läbiviimisel õigus (KKS § 41[5] lg 1):

1) pöörduda riigi ja kohaliku omavalitsuse üksuse asutuste ja ametiisikute, samuti füüsiliste ja juriidiliste isikute poole järelepärimisega kontrollitava isikuandmete kohta;
2) vestelda kontrollitava, samuti tema tööandja või õppeasutuse esindajate ning teiste isikutega, et selgitada välja kontrollitava kõlbelisi ja teisi isiksuseomadusi ning vajaduse korral ja küsitletava isiku nõusolekul võtta temalt kirjalik seletus;
3) kontrollida, kas kontrollitavat on karistatud kuriteo eest, kas kontrollitav on kandnud vabadusekaotuslikku karistust või kas ta on kriminaalmenetluses kahtlustatav või süüdistatav;
4) kontrollida isikuandmeid riigi, kohaliku omavalitsuse või muu avalik-õigusliku juriidilise isiku või eraõigusliku juriidilise isiku andmekogust;
5) saada andmeid karistusregistri arhiivist.

3.3. Protseduurid põhiõiguste riive õiguspärasuse tagamiseks

3.3.1. Teabeamet

Luure ja vastuluure teostamisel on Teabeametil kohustus lähtuda järgmistest üldistest põhimõtetest:

[34] Variisik KKS tähenduses on tegevväelane, kes teenistussuhte varjamise või muudetud identiteedi abil aitab tagada teesklemise varjatust (KKS § 37[3] lg 2).
[35] Kaitseväe korralduse seaduse muutmise seaduse eelnõu seletuskiri, lk 3.

1) teavet, sealhulgas isikuandmeid, võib koguda ja töödelda siis, kui see on vajalik Teabeameti ülesannete täitmiseks (JAS § 3 lg 1);
2) oma ülesannete täitmiseks võib kasutada ainult vajalikke abinõusid. Mitme võimaliku abinõu olemasolul tuleb kasutada sellist, mis isikute põhiõigusi seoses julgeolekuasutuse ülesande täitmisega võimalikult vähe piirab. Kasutada võib abinõu, mis ei piira üksikisiku põhiõigusi ülemääraselt, võrreldes taotletava eesmärgiga (proportsionaalsuse põhimõte) (JAS § 3 lg 2);
3) teabe kogumine ei tohi kahjustada isiku elu, tervist, vara ega keskkonda (JAS § 24 lg 2).

Lisaks üldistele põhimõtetele, näeb JAS ette protseduurid vastavalt sellele, millist meedet kasutatakse. Postisaadetise läbivaatus, elektroonilise side võrgu kaudu edastatava sõnumi või muu teabe või muul viisil edastatava teabe pealtkuulamine, -vaatamine või salvestamine võib toimuda üksnes halduskohtu loal (JAS § 27 lg 1). Ka varjatult sisenemine ruumi, hoonesse, piirdega alale, sõidukisse või arvutisüsteemi teabe varjatud kogumiseks, salvestamiseks või selleks vajalike tehniliste abivahendite paigaldamiseks ja eemaldamiseks võib toimuda halduskohtu loal (JAS § 27 lg 1).

Loa saamiseks esitab julgeolekuasutuse juht halduskohtu esimehele või tema määratud halduskohtunikule põhjendatud kirjaliku taotluse. Kohus võib sealjuures nõuda täiendavate tõendite või seletuste esitamist (JAS § 27 lg 2, HKMS § 264 lg 2). Loa võib anda kuni kaheks kuuks või pikendada iga kord sama tähtaja võrra.

Kõigi kodu, perekonna- või eraelu puutumatust piiravate meetmete kasutamise, v.a eelnevalt nimetatud meetmed, otsustab Teabeameti juht või tema poolt volitatud ametnik korraldusega (JAS § 27 lg 3). See korraldus kehtib selles märgitud tähtaja jooksul, kuid mitte kauem kui kaks kuud.

Isikute teavitamine kasutatud vahenditest

JAS § 29 alusel on julgeolekuasutusel kohustus teavitada isikut, kelle sõnumi saladust ja kodu, perekonna- või eraelu puutumatuse õigust on piiratud JAS §-s 25 või 26 sätestatud viisil, kasutatud abinõudest ja põhiõiguste piiramise asjaoludest viivitamatult, kui see ei ohusta piirangu eesmärki, või sellise ohu lõppemisel. Seetõttu on julgeolekuasutusel küll kohustus isiku teavitada, kuid kui see ohustab menetlust, võib isiku teavitamise edasi lükata.

Julgeolekukontrolli tegemine RSVS alusel

Julgeolekukontrolli võib teostada üksnes juhul, kui isik on selleks andnud nõusoleku (RSVS § 47 lg 6). Julgeolekukontrolli teostaval asutusel on õigus RSVS §-s 32 ja § 42 lõigetes 2 ja 3 nimetatud asjaolude esinemist kontrollida ka juurdepääsuloa ja juriidilise isiku töötlemisloa kehtivusajal ning viie aasta jooksul pärast selle kehtivuse lõppemist, kui isik on loa kehtivuse ajal kokku puutunud salastatud teabega, mille avalikuks tulek kahjustaks oluliselt riigi julgeolekut. Kuivõrd julgeolekukontrollis on lubatud kasutada kõiki JAS-is sätestatud vastuluure meetmeid, kohalduvad nende meetmete rakendamisele eeltoodud JAS-st tulenevad põhimõtted ning protseduurid.

Pangasaladusele ligipääsu saamiseks esitab Teabeamet järelepärimise kirjalikus või elektroonilises vormis KAS-s nõutud andmetega (KAS § 88 lg 5, 6).

3.3.2. Kaitsepolitseiamet

(a) Protseduurid õiguspärasuse tagamiseks vastuluure valdkonnas

KAPO-l on vastuluure valdkonnas võimalik kasutada meetmeid nii JAS kui ka PPVS alusel. JAS alusel sätestatud meetmed ja protseduurid on sisuliselt samad, mis Teabeametil, mida käsitleti eelmises alapunktis (3.3.1.). Seetõttu käsitletakse käesolevas osas üksnes PPVS-s ja julgeolekukontrollis kasutatavaid meetmeid.

Politsei ja piirivalve seaduses sätestatud meetmete kasutamine

Päringu tegemine elektroonilise side ettevõtjale on lubatud PPVS alusel üksnes kuriteo ettevalmistamise avastamiseks või tõkestamiseks ning tagaotsitavaks kuulutamise määruse täitmiseks. Päringu võib teha

üksnes isiku suhtes, kelle puhul on põhjendatult alust arvata, et ta paneb toime kuriteo (KrMS § 126^2 lg-s 2 sätestatud kuriteo) või kes on kuulutatud tagaotsitavaks (PPVS § 7^{49}).

Sõltuvalt taotletavate andmete sisust toimub andmetele ligipääsu saamine kahel viisil. Nn omanikupäringu[36] tegemiseks seadus loa taotlemise protseduuri ette ei näe. Samas muu kui omanikupäringu (andmed sõnumi edastamise fakti kohta) tegemiseks sideettevõtjale annab loa prokuratuur. Milliseid asjaolusid ja kaalutlusi peab prokuratuur loa andmiseks arvestama, seda seadus ette ei näe. Seadus näeb ette üksnes selle, et prokuratuur peab märkima kuupäevalise täpsusega ajavahemiku, mille kohta andmete nõudmine on lubatud (PPVS § 7^{49} lg 2).

Politsei võib kasutada salajasele koostööle kaasatud isikut jälitustoimingute tegemise tagamiseks või teabe kogumiseks. Loa isiku kaasamiseks annab KAPO peadirektor või tema volitatud ametnik (PPVS § 7^{51} lg 3, JAS § 21 lg 3).

Konspiratsioonivõtete teostamise otsustab KAPO peadirektor või tema volitatud ametnik (PPVS § 7^{54}). Konspiratsioonivõtte kasutamiseks esitatakse vajadusel põhjendatud taotlus haldusorganile või juriidilisele isikule, kes annab välja vajaliku dokumendi ning teeb vajaliku muudatuse andmekogus või registris.

Teeseldava eraõigusliku juriidilise isiku või välisriigi äriühingu filiaali asutamiseks või soetamiseks esitab KAPO vastutavale ministrile taotluse kirjaliku nõusoleku saamiseks (PPVS § 7^{55} lg 2 ja 3). Taotlus peab olema põhistatud, näidates ära isiku teesklemise vajaduse, teeseldava isiku liigi, kulud ning teesklemise kestuse, kui see on kindlaks määratav (PPVS § 7^{55} lg 3).

Variisikut võib kasutada jälitustoimingute tegemiseks, jälitustoimingute tegemise tagamiseks või teabe kogumiseks (PPVS § 7^{56} lg 1). Selle meetme kasutamiseks annab loa KAPO peadirektor (PPVS § 7^{56} lg 3, JAS § 21 lg 3).

Isiku teavitamine ja kogutud andmete tutvustamine PPVS alusel tehtud jälitustoimingust

Isiku võib jätta tema suhtes tehtud jälitustoimingust teavitamata KAPO peadirektori või tema volitatud ametniku loal järgmistel juhtudel (PPVS §7^{58} lg 1, KrMS § 126^{13} lg 2):

1) teavitamine võib kahjustada oluliselt kriminaalmenetlust;
2) teavitamine võib kahjustada oluliselt teise isiku seadusega tagatud õigusi ja vabadusi või seada teise isiku ohtu;
3) teavitamine võib seada ohtu jälitusasutuse meetodite, taktika, jälitustoimingu tegemisel kasutatava vahendi või politseiagendi, variisiku või salajasele koostööle kaasatud isiku koostöö salajasuse.

Isikule võib jätta tutvustamata kuni vastava aluse äralangemiseni jälitustoiminguga kogutud andmed (PPVS §7^{58} lg 1, KrMS § 126^{14} lg 1):

1) teiste isikute perekonna- või eraelu kohta;
2) mille tutvustamine võib kahjustada teise isiku seadusega tagatud õigusi ja vabadusi;
3) mis sisaldavad riigisaladust või salastatud välisteavet või teise isiku seadusega kaitstud saladusi;
4) mille tutvustamine võib seada ohtu jälitusasutuse töötaja, politseiagendi, variisiku, salajasele koostööle kaasatud isiku või jälitustoimingus osalenud muu isiku või nende lähikondsete elu, tervise, au, hea nime või vara;
5) mille tutvustamine võib seada ohtu politseiagendi, variisiku ja salajasele koostööle kaasatud isiku õiguse hoida koostööd saladuses;
6) mille tutvustamise tulemusena võidakse edastada teavet jälitusasutuse meetodite, taktika ja jälitustoimingu tegemisel kasutatava vahendi kohta;
7) mida ei ole võimalik eraldada ja esitada selliselt, et neist ei ilmneks andmed, mis on loetletud eelmistes punktides.

[36] elektroonilise side võrgus kasutatavate identifitseerimistunnustega seotud lõppkasutaja tuvastamiseks vajalikud andmed.

Seega, kui ei esine eelnimetatud aluseid, tuleks isikut teavitada teostatud jälitustoimingust ning lubada kogutud andmetega tutvuda. Vastavalt PPVS alusel kehtestatud korrale (siseministri 25.02.2013 määrus nr 7 „Politsei ja piirivalve seaduse alusel tehtud jälitustoiminguga kogutud teabe vormistamise ja säilitamise ning jälitustoimingust teavitamise ja jälitustoiminguga kogutud andmete tutvustamise kord“) teavitatakse isikut pärast tema kohta jälitusteabele juurdepääsu otsustamist (§ 3 lg 1).

Julgeolekukontrolli tegemine RSVS alusel

Julgeolekukontrolli võib teostada üksnes juhul, kui isik on selleks andnud nõusoleku (RSVS § 47 lg 6). Julgeolekukontrolli teostaval asutusel on õigus RSVS §-s 32 ja § 42 lõigetes 2 ja 3 nimetatud asjaolude esinemist kontrollida ka juurdepääsuloa ja juriidilise isiku töötlemisloa kehtivusajal ning viie aasta jooksul pärast selle kehtivuse lõppemist, kui isik on loa kehtivuse ajal kokku puutunud salastatud teabega, mille avalikuks tulek kahjustaks oluliselt riigi julgeolekut. Kuivõrd julgeolekukontrollis, sh erisubjektide üle, on lubatud kasutada kõiki JAS-is sätestatud vastuluure meetmeid, kohalduvad nende meetmete rakendamisele eeltoodud JAS-st tulenevad põhimõtted ning protseduurid.

Pangasaladusele ligipääsu saamiseks esitab KAPO järelepärimise kirjalikus või elektroonilises vormis KAS-s nõutud andmetega (KAS § 88 lg 5, 6).

(b) Protseduurid õiguspärasuse tagamiseks korrakaitse valdkonnas

Kriminaalmenetluse seaduse alusel teostatavad jälitustoimingud

KrMS näeb ette mitmed üldpõhimõtted, mille järgimine peaks tagama põhiõiguste riive õiguspärasuse:

1) jälitustoiming on lubatud üksnes juhul, kui andmete kogumine muude toimingutega või tõendite kogumine muude menetlustoimingutega ei ole võimalik, ei ole õigel ajal võimalik või on oluliselt raskendatud või kui see võib kahjustada kriminaalmenetluse huve (nn *ultima ratio* põhimõte (KrMS § 126^1 lg 2);
2) jälitustoiminguga ei või ohustada isiku elu ja tervist, põhjendamatult ohustada vara ja keskkonda ega põhjendamatult riivata muid isikuõigusi (KrMS § 126^1 lg 3);
3) jälitustoimingu aluse äralangemise korral tuleb jälitustoiming viivitamata lõpetada (KrMS § 126^2 lg 9);

KrMS-s sätestatud jälitustoiminguid võib kasutada teabe kogumiseks kuriteo ettevalmistamise kohta selle avastamise või tõkestamise eesmärgil üksnes KrMS § 126^2 lg 2 nimetatud kuritegude puhul. Vaadata varjatult läbi postisaadetist, vaadata või kuulata salaja pealt teavet või kasutada politseiagenti võib üksnes KarS §-des 244^{37} ja 246^{38}, § 266 lõike 2 punktis 3^{39} ning §-des 255^{40} ja 256^{41} nimetatud kuriteo ettevalmistamise kohta teabe kogumisel (KrMS 126^3 lg 2). Seega on KAPO volitused kasutada jälitustoiminguid piiratud konkreetsete kuritegudega.

Samuti piiritleb KrMS need isikud, kelle suhtes on jälitustoiminguid lubatud teha. KrMS alusel võib jälitustoimingut teha üksnes isiku suhtes, kelle puhul on põhjendatult alust arvata, et ta paneb toime KrMS § 126^2 lg-s 2 nimetatud kuriteo (KrMS § 126^2 lg 3).

Jälitustoiminguga kaasneva põhiõiguse riive õiguspärasuse suurimaks garantiiks on see, et jälitustoimingut on lubatud teha üksnes prokuratuuri või eeluurimiskohtuniku kirjalikul loal (KrMS 126^4 lg 1). Loa saamiseks eeluurimiskohtunikult peab prokuratuur esitama põhjendatud taotluse (KrMS § 126^4 lg 1). Teatud juhtudel on loa nõudest võimalik kõrvale kalduda. Näiteks edasilükkamatul juhul võib prokuratuuri luba nõudva jälitustoimingu teha prokuratuuri loal, mis on antud taasesitamist võimaldaval viisil (KrMS 126^4 lg 2). Sellisel juhul vormistatakse kirjalik luba 24 tunni jooksul jälitustoimingu alustamisest arvates.

[37] Rünne kõrge riigiametniku elule ja tervisele
[38] Rünne rahvusvaheliselt kaitstud isiku elule ja tervisele
[39] Omavoliline sissetung diplomaatilise puutumatusega maa-alale, hoonesse, ruumi.
[40] Kuritegelikku ühendusse kuulumine.
[41] Kuritegeliku ühenduse organiseerimine.

Samuti, kui tegemist on vahetu ohuga isiku elule, kehalisele puutumatusele, füüsilisele vabadusele või suure väärtusega varalisele hüvele ning loa taotlemine või vormistamine ei ole õigel ajal võimalik, võib kohtu luba nõudva jälitustoimingu teha edasilükkamatul juhul kohtu loal, mis on antud taasesitamist võimaldaval viisil (KrMS 126^4 lg 2). Kirjalik taotlus ning luba vormistatakse 24 tunni jooksul jälitustoimingu alustamisest arvates.

Põhiõiguste riive õiguspärasuse tagamiseks piirab KrMS ka jälitustoimingute kestust. Nimelt ei tohi jälitustoimingu kestus konkreetse isiku suhtes samas menetluses ületada ühte aastat (KrMS § 126^4 lg 6). Erandjuhul võib riigi peaprokurör siiski anda loa või taotleda kohtult luba jälitustoimingu tegemiseks isiku suhtes kestusega üle ühe aasta. Millised need erandjuhud on, seadus ei täpsusta.

See, kas jälitustoiming nõuab eeluurimiskohtuniku või prokuratuuri luba, sõltub jälitustoimingu liigist. Näiteks varjatud jälgimise, võrdlusmaterjali varjatud kogumise ja esmauuringute tegemise, asja varjatud läbivaatuseks ja asendamiseks on vajalik prokuratuuri luba (KrMS § 126^5 lg 1). Loa võib anda kuni kaheks kuuks ning seda võib pikendada kuni kahe kuu kaupa.

Postisaadetise varjatud läbivaatuseks ning teabe salajaseks pealtkuulamiseks või –vaatamiseks annab loa eeluurimiskohtunik (KrMS § 126^6 lg 3, § 126^7). Luba antakse kuni kaheks kuuks ning seda võib pikendada kuni kahe kuu kaupa.

Politseiagendi kasutamiseks annab kirjaliku loa prokuratuur (KrMS § 126^9 lg 2). Luba antakse kuni kuueks kuuks ning seda võib pikendada korraga kuni kuue kuu võrra.

Eelnevale lisaks näeb KrMS ette ka reeglid jälitustoiminguga saadud andmete dokumenteerimisele, säilitamisele, kasutamisele ja hävitamisele (KrMS § 126^{10-12}).

Jälitustoimingust teavitamine

Jälitustoimingu tegemise loa tähtaja lõppemise korral peab KAPO isikut, kelle suhtes jälitustoiming tehti või kelle perekonna- või eraelu puutumatust riivati, viivitamata jälitustoimingust teavitama (KrMS § 126^{13} lg 1). Teavitamata jätmine on samas lubatud prokuratuuri loal, siis kui teavitamine võib:

1) kahjustada oluliselt kriminaalmenetlust;
2) kahjustada oluliselt teise isiku seadusega tagatud õigusi ja vabadusi või seada teise isiku ohtu;
3) seada ohtu jälitusasutuse meetodite, taktika, jälitustoimingu tegemisel kasutatava vahendi või politseiagendi, variisiku või salajasele koostööle kaasatud isiku koostöö salajasuse (KrMS § 126^{13} lg 2).

Teavitamata võib jätta üksnes eelnevalt nimetatud aluse äralangemiseni. Sealjuures on prokuratuuril kohustus kontrollida teavitamata jätmise aluse olemasolu kriminaalasjas kohtueelse menetluse lõppemisel, kuid mitte hiljem kui üks aasta pärast jälitustoimingu loa tähtaja lõppemist (KrMS § 126^{13} lg 3). Juhul, kui alus ära ei lange, peab prokuratuur taotlema eeluurimiskohtunikult luba teavitamata jätmise tähtaja pikendamiseks. Eeluurimiskohtunik võib otsustada teavitamata jätmise tähtajatu või tähtajalisena (KrMS § 126^{13} lg 4). Teavitamata jätmise loa tähtaja lõppemise või selle pikendamisest keeldumise korral teavitatakse isikut jälitustoimingust viivitamata.

Prokuratuuri otsusel jäetakse politseiagendi kasutamise fakt või politseiagendi isik salastatuks ka pärast jälitustoimingu lõpetamist, kui avalikustamine võib seada ohtu politseiagendi või tema lähikondsete elu, tervise, au või hea nime või vara või tema edasise tegutsemise politseiagendina (KrMS § 126^9 lg 5).

Korrakaitseseaduse alusel rakendatavad riikliku järelevalve meetmed

Riikliku järelevalve meetmete rakendamisel on kohustus lähtuda järgmistest põhimõtetest (KorS § 7):

1) kohaldada tuleb mitmest sobivast ja vajalikust riikliku järelevalve meetmest seda, mis nii isikut kui ka üldsust eeldatavalt kõige vähem kahjustab;
2) kohaldada võib ainult sellist riikliku järelevalve meedet, mis on proportsionaalne, arvestades meetmega taotletavat eesmärki ja kiireloomulist kohaldamist nõudvat olukorda, ja
3) kohaldada võib riikliku järelevalve meedet vaid nii kaua, kui selle eesmärk on saavutatud või seda ei ole enam võimalik saavutada.

Riikliku järelevalve meetmeid võib rakendada nii isiku suhtes, kes on avaliku korra eest vastutav (isik, kes on põhjustanud ohukahtluse või ohu, KorS § 15 lg 1, § 23 lg 1) kui ka isiku suhtes, keda ei ole alust pidada avaliku korra eest vastutavaks isikuks (KorS § 25 lg 1). Üldreeglina ei ole nende meetmete kasutamise eelduseks loa taotlemine.

Juhul kui aga riikliku järelevalve meetmeid soovitakse kasutada muu isiku kui avaliku korra eest vastutava isiku suhtes, peab KAPO taotlema asjaomaselt ministrilt eelneva kirjaliku loa järgmiste meetmete kasutamiseks: isiku samasuse tuvastamiseks eriliste tuvastusmeetmetega, sõiduki peatamiseks, turvakontrolli teostamiseks, vallasasja läbivaatuseks ning isiku läbivaatuseks ja valdusesse sisenemiseks (KorS § 26 lg 1 ja 2).[42] Edasilükkamatutel juhtudel võib neid teha ka ilma ministri loata või suulise loa alusel, mis tuleb 24 tunni jooksul kirjalikuks loaks vormistada (KorS § 25 lg 3 ja 5).

Vahetu sunni kohaldamise eelduseks on reeglina eelneva kohustava haldusakti andmine. Haldussunni kasutamine on sellisel juhul lubatud siis, kui ohu väljaselgitamine, tõrjumine või korrarikkumise kõrvaldamine ei ole muul viisil või õigel ajal võimalik (KorS § 76 lg 1). Vahetut sundi on võimalik siiski kohalda ilma eelneva haldusaktita, kui esineb kiire vajadus vahetu kõrgendatud ohu tõrjumiseks või korrarikkumise kõrvaldamiseks (KorS § 76 lg 2).

Elektroonilise side andmete pärimine sideettevõtjalt ning mobiiltelefonivõrgus kasutatavate terminalseadmete asukoha tuvastamine reaalajas on lubatud üksnes isiku suhtes, kelle puhul see on vajalik kõrgendatud ohu väljaselgitamiseks või tõrjumiseks (KorS § 35 lg 1). Päringu võib sideettevõtjale teha üksnes kirjalikult või elektrooniliselt. Nende meetmete rakendamine tuleb igal juhul protokollida ning nendest tuleb isikut viivitamatult teavitada (KorS § 35 lg 2 ja 3).

Valdusesse sisenemine ja selle läbivaatus on lubatud siis kui:

1) see on vajalik kõrgendatud ohu väljaselgitamiseks või tõrjumiseks;
2) on alust arvata, et piiratud või tähistatud kinnisasjal, ehitises või ruumis viibib isik, kellelt võib võtta seaduse alusel vabaduse või kelle elu, tervis või kehaline puutumatus on tingituna tema abitust seisundist ohustatud;
3) see on vajalik seadusega või seaduse alusel kehtestatud nõuete täitmise tagamisel ohu ennetamiseks, väljaselgitamiseks või tõrjumiseks või korrarikkumise kõrvaldamiseks, ning selliste nõuete täitmise tagamine on valdusesse siseneva korrakaitseorgani pädevuses (KorS § 50 lg 1 ja § 51 lg 1).

Valdusesse sisenemisel, juhul kui isikut ennast juures ei viibi, tuleb esimesel võimalusel teavitada isikut valdusesse sisenemisest (KorS § 50 lg 5).

Üksikasjalised tingimused, millal ja kuidas on riikliku järelevalve meetmete kui ka vahetu sunni kohaldamine lubatud, sätestab korrakaitseseadus.

Politsei ja piirivalve seaduses sätestatud meetmete kasutamine

PPVS alusel sätestatud meetmed kasutamise protseduure kirjeldati eelnevas alapeatükis *Protseduurid õiguspärasuse tagamiseks korrakaitse valdkonnas*.

(c) Süütegude menetlemise ülesanded

KrMS-s sätestatud jälitustoimingute kasutamist käsitleti eelnevas alapeatükis *Korrakaitselised ülesanded*. KAPO võib KrMS § 126^2 lõike 1 punktis 4 nimetatud alusel kuriteo avastamise või kurjategija kinnipidamise eesmärgil matkida kuritegu (KrMS § 126^3 lg 3). Kuriteo matkimine toimub eeluurimiskohtuniku loal (KrMS § § 126^8). Luba antakse kuni kaheks kuuks ja seda võib pikendada kuni kahe kuu kaupa.

Kriminaalmenetluse raames on võimalik elektroonilise side andmete nõudmine sideettevõtjalt (KrMS § 90^1). Menetlejal on õigus teha nn omaniku päringuid. Muu kui omaniku päringute puhul (st

[42] isiku läbivaatus ja valdusesse sisenemine on sealjuures lubatud üksnes siis kui see on vajalik isiku elu või kehalise puutumatusele ähvardava ohu väljaselgitamiseks.

sõnumi edastamise fakti kohta) võib uurimisasutus teha üksnes prokuratuuri loal kohtueelses menetluses või kohtu loal kohtumenetluses. Päringu võib teha üksnes siis, kui see on vältimatult vajalik kriminaalmenetluse eesmärgi saavutamiseks. Päringu tegemise loas märgitakse kuupäevalise täpsusega ajavahemik, mille kohta andmete nõudmine on lubatud.

Posti- või telegraafisaadetise arest ja läbivaatus toimub prokuratuuri taotlusel eeluurimiskohtuniku määruse või kohtumääruse alusel (KrMS § 89 lg 1).

Läbiotsimist võib toimetada prokuratuuri taotlusel eeluurimiskohtuniku määruse või kohtumääruse alusel (KrMS § 91 lg 2). Nii eeluurimiskohtuniku määrus kui ka kohtumäärus prokuratuuri läbiotsimistaotluse lahendamise kohta võib olla koostatud pealdisena prokuratuuri taotlusel. Edasilükkamatul juhul, kui läbiotsimismääruse vormistamine ei ole õigel ajal võimalik, võib toimetada läbiotsimist prokuratuuri loa alusel, mis on antud taasesitamist võimaldaval viisil (KrMS § 91 lg 5). Eelnevat ei pea järgima, kui see on vajalik:

1) laiba või sündmuskoha vaatluseks vahetult laiba leidmise või kuriteo toimepanemise järel või
2) isiku kahtlustatavana kinnipidamiseks vahetult pärast kuriteo toimepanemist (KrMS § 91^1).

Vaatluseks, isiku läbivaatuseks ning uurimiseksperimendiks ei ole vaja prokuratuuri ega kohtu luba.

Väärteomenetluse raames korruptsioonivääreteo uurimiseks võib KAPO taotleda kohtult sellise määruse andmist, millega võimaldatakse juurdepääs pangasaladusele ja fondiosakute registri andmetele (VTMS § 31 lg 3). Selle meetme kasutamine peab aga olema vältimatult vajalik korruptsioonivääreteo menetluse eesmärgi saavutamiseks (nn *ultima ratio* põhimõte).

Elektroonilise side omanikupäringu puhul ei ole loamehhanismi sätestatud, kuid muu kui omanikupäringu puhul võib KAPO teha kohtu loal üksikpäringu[43] (VTMS § 31^2 lg 1 ja 2). Päringu võib teha üksnes siis, kui see on vältimatult vajalik väärteomenetluse eesmärgi saavutamiseks (VTMS § 31^2 lg 3). KAPO võib väärteomenetluses läbi otsida oma määruse alusel, millel on resolutsioonina maakohtuniku luba (VTMS § 35 lg 1).

3.3.3. Kaitsevägi

Kaitsevägi võib kaasata isikut salajasse koostöösse (KKS § 37^1 lg 1), teeselda eraõiguslikku juriidilist isikut, tema struktuuriüksust või organit või äriühingu filiaali (KKS § 37^2 lg 1) ning kasutada variisikut (KKS § 37^3 lg 1) üksnes järgmistel juhtudel:

1) rahvusvahelise sõjalise operatsiooni piirkonnas sõjalise operatsiooni ettevalmistamiseks;
2) rahvusvahelise sõjalise operatsiooni piirkonnas sõjalise operatsiooni läbiviimiseks;
3) sõjalises operatsioonis osaleva Kaitseväe üksuse kaitseks;
4) väljaspool Eesti Vabariigi territooriumi tegutsemiseks vajaliku teabe kogumiseks.

Väljaspool Eesti Vabariigi territooriumi tegutsemiseks isikute küsitlemisel, isiku kaasamisel salajasele koostööle ning eraõigusliku juriidilise isiku, tema struktuuriüksuse, organi või äriühingu filiaali teesklemisel ja variisiku kasutamisel ei või Kaitsevägi koguda ega töödelda teavet Eesti kodaniku kohta (KKS § 37 lg 2^1).

Isiku kaasamine salajasse koostöösse ja variisiku kasutamine toimub Kaitseväe põhimääruses määratud Kaitseväe struktuuriüksuse ülema kirjaliku loa alusel. Teeseldava isiku või äriühingu filiaali asutamise või soetamise otsustab kaitseminister.

Teabeamet annab Kaitseväele abi juhul, kui teabe kogumine muul õiguspärasel viisil ei ole võimalik või oleks ebaproportsionaalselt raske ning kogutav teave on riigi sõjaliseks kaitsmiseks vältimatult vajalik

[43] Üksikpäring on kirjalik päring elektroonilise side seaduse § 111^1 lõigetes 2 ja 3 nimetatud andmete saamiseks konkreetse telefonikõne, elektronkirja, elektroonilise kommentaari või muu üksiksõnumi edastamisega seotud sideseansi kohta

(KKS § 39 lg 2). Teabeamet esitab Kaitseministeeriumile iga nelja kuu järel kirjaliku ülevaate Kaitseväe juhataja taotlusel rakendatud volituste ja nendega saadud andmete kohta (KKS § 39 lg 3).

Päringu tegemine elektroonilise side ettevõtjale on lubatud KKS § 41^1 alusel üksnes kuriteo ettevalmistamise avastamiseks või tõkestamiseks ning tagaotsitavaks kuulutamise määruse täitmiseks. Päringu võib teha üksnes isiku suhtes, kelle puhul on põhjendatult alust arvata, et ta paneb toime kuriteo (KrMS § 126^2 lg-s 2 sätestatud kuriteo) või kes on kuulutatud tagaotsitavaks.

Sõltuvalt taotletavate andmete sisust toimub andmetele ligipääsu saamine kahel viisil. Nn omanikupäringu[44] tegemiseks seadus loa taotlemise protseduuri ette ei näe. Samas muu kui omanikupäringu (andmed sõnumi edastamise fakti kohta) tegemiseks sideettevõtjale annab loa prokuratuur. Milliseid asjaolusid ja kaalutlusi peab prokuratuur loa andmiseks arvestama, seda seadus ette ei näe. Seadus näeb ette üksnes selle, et prokuratuur peab märkima kuupäevalise täpsusega ajavahemiku, mille kohta andmete nõudmine on lubatud (KKS § 41^1 lg 2).

Jälitusteabele juurdepääsu andmisel KrMS § 126^3 lõikes 1 nimetatud jälitustoimingute tegemiseks ning elektroonilise side meta-andmete kogumiseks peab olema isiku, kelle kohta andmeid kogutakse, eelnev kirjalik nõusolek (KKS § 41^2 lg 2).

Taustakontrolli teostamiseks peab samuti olema isiku eelnev kirjalik nõusolek, millega isik lubab Kaitseväel koguda enda kohta andmeid 5 aasta jooksul (KKS § 41^6). Kaitsevägi võib andmeid koguda Kaitseväkke teenistusse või tööle kandideerimisel ja iga viie aasta järel pärast isiku Kaitseväkke teenistusse või tööle võtmist Kaitseväkke sobivuse hindamisel (KKS § 41^8). Põhjendatud vajaduse korral võib andmeid koguda ka muul ajal, kui on tekkinud põhjendatud kahtlus, et isiku kohta on teenistuse või tööloleku ajal ilmnenud asjaolud, mis välistaksid teenistusse või töölevõtmise. Isiku kohta taustakontrolli käigus kogutud andmeid säilitatakse tema teenistuse ja töölepingu kehtivuse ajal ning kolm aastat pärast tema teenistusest vabastamist või töölepingu lõppemist toimikus, mis on kaitstud mitteõiguspärase juurdepääsu eest (KKS § 41^{10} lg 2). Taustakontrolli käigus kogutud isikuandmeid võib edastada avaliku teabe seaduses sätestatud korras riigiasutustele ainult tausta- või julgeolekukontrolli eesmärgil (KKS § 41^{10} lg 3).

Isiku teavitamine

Kaitsevägi teavitab isikut kasutatud abinõudest ja põhiõiguste piiramise asjaoludest viivitamata, kui see ei ohusta piirangu eesmärki, või sellise ohu lõppemisel, järgmistel juhtudel (KKS § 40):

1) isiku põhiõigusi on piiratud kogudes või töödeldes väljaspool üldkasutatavat Eesti Vabariigi territooriumil asuvat elektroonilise side võrku edastatavaid või levivaid signaale;
2) isiku põhiõigusi on piiratud JAS §-des 23, 25 ja 26 sätestatud volituste rakendamisega.

Juhul kui jälitusteabele juurdepääsu võimaldamiseks on isiku kohta kogutud andmeid jälitustoiminguga või tehtud päring sideettevõtjale, teavitatakse seda isikut toimingu tegemisest ning vajadusel tutvustatakse kogutud andmeid (KKS § 41^2 lg 3).

3.4. Järelevalve korraldus julgeoleku- ja luureasutuste tegevuse õigus- ja eesmärgipärasuse üle

Eesti õigussüsteem näeb julgeolekuasutuste järelevalves ette erinevaid järelevalve protseduure, nii *ex ante* kui ka *ex post* protseduure. Eelnevas osas käsitleti juba *ex ante* järelevalve protseduure (nt teatud juhtudel kohtuliku loa küsimine) ning *ex post* järelevalve protseduurina isiku teavitamist, mistõttu neid käesolevas osas kordama ei hakata ning keskendutakse ülejäänud *ex post* järelevalve protseduuridele.

(a) Teenistuslik järelevalve

[44] Elektroonilise side võrgus kasutatavate identifitseerimistunnustega seotud lõppkasutaja tuvastamiseks vajalikud andmed.

Teabeameti üle teostab teenistuslikku järelevalve Kaitseministeerium (VVS § 60).

KAPO üle teostab teenistuslikku järelevalvet Siseministeerium (VVS § 66 lg 2).

Kaitseväe üle teostab teenistuslikku järelevalvet valdkonna eest vastutav minister ehk kaitseminister (KKS § 7 lg 1). Kaitseväe sees teostab teenistuslikku järelevalve Kaitseväe juhataja (KKS § 7 lg 2). Juhul kui Kaitsevägi küsitleb isikuid, kaasab isikuid salajasse koostöösse või teeskleb eraõiguslikku juriidilist isikut, tema struktuuriüksust, organit või äriühingu filiaali või kasutab variisikut väljaspool Eesti Vabariigi territooriumi tegutsemiseks, teavitatakse sellest riigikaitse valdkonna eest vastutavat ministrit ehk kaitseministrit tema kehtestatud korras[45] (KKS § 42 lg 4).

Kaitsevägi esitab Kaitseministeeriumile iga 4 kuu järel kirjaliku ülevaate kaitseväeluure teostamisel kogutud andmete ja nende saamiseks kasutatud vahendite ja meetmete kohta ning iga 6 kuu järel ülesannete täitmise aruande (KKS § 43 lg 2).

(b) Prokuratuur

Prokuratuur teostab KrMS (§ 126[15] lg 1) alusel järelevalvet jälitustoimingu vastavuse üle jälitustoiminguks antud loale. Prokuratuuril on jälitusasutuse tegevuse üle järelevalve teostamiseks õigus tutvuda sõnumi ülekandmise taotlustega ja sõnumi tsentraliseeritud jälgimisseadmesse ülekandmise korral säilinud logifailidega (ESS § 113 lg 8).

(c) Riigikogu julgeolekuasutuste järelevalve komisjon

Teabeameti ja KAPO üle teostab järelevalvet Riigikogu julgeolekuasutuste järelevalve komisjon (JAS § 36). Julgeolekuasutuste järelevalve komisjon teostab lisaks järelevalvet ka jälitusametkondade üle KrMS alusel tehtud jälitustoimingute osas (§ 126[15] lg 2) ning kaitseväeluure teostamise üle (KKS § 42 lg 1). Julgeolekuasutuste järelevalve komisjon on Riigikogu erikomisjon, kelle pädevuses on kontrollida nii põhiõiguste tagamist kui ka asutuste tegevuse tõhusust (JAS § 36 lg 1).

Julgeolekuasutuste järelevalve komisjoni järelevalve toimib selliselt, et peaminister ja asjaomane minister teavitavad komisjoni julgeolekuasutuste ja jälitusametkondade tegevusest ja järelevalvest nende tegevuse üle, sealhulgas esitavad vähemalt kord kuue kuu jooksul ülevaate nimetatud küsimustes (JAS § 36 lg 2). Lisaks ülevaadete saamisele on komisjonil õigus välja kutsuda isikuid ja nõuda tutvumiseks dokumente (JAS § 36 lg 3). Komisjonil on õigus tutvuda elektroonilise side ettevõtja poolt säilitatud sõnumi ülekandmise taotlustega ja sõnumi tsentraliseeritud jälgimisseadmesse ülekandmise korral säilinud logifailidega (ESS § 113 lg 8).

Oma tegevuste ja tulemuste kohta esitab komisjon vähemalt kord aastas Riigikogule ülevaate (JAS § 36 lg 5), mis reeglina ka avalikustatakse. Juhul kui komisjon avastab seaduserikkumise, on komisjon kohustatud edastama materjalid uurimisasutusele või õiguskantslerile (JAS § 36 lg 6).

Julgeolekuasutuste järelevalve komisjoni töö osas on avaldatud kahtlust, kas sellel komisjonil on piisavalt pädevust ning ressursse tõhusaks kontrolliks.[46] Tegelikkuses sõltub järelevalve erikomisjoni liikmete tahtest ja tõlgendustest.[47] Samuti on märgitud, et Riigikogu komisjonil võiks lisaks formaalsele ärakuulamiskohustusele olla oluliselt aktiivsem roll, näiteks juhiste või suuniste väljatöötamise õigus. [48]

(d) Õiguskantsler

Alates 01.01.2015 teostab õiguskantsler järelevalvet põhiõiguste ja -vabaduste järgimise üle täidesaatva riigivõimu asutuste poolt varjatult isikuandmete ja nendega seonduva teabe kogumise, töötlemise,

---

[45] Seda korda minister kehtestanud ei ole.

[46] U. Lõhmus. Pealtkuulamine ja Eesti põhiseaduses sätestatud õigus sõnumite saladusele. – Juridica 2008/VII, lk 472. E. Sisas. Julgeolekusektori parlamentaarne järelevalve Eestis. Riigikogu Toimetised 2015(31). Kättesaadav: http://www.riigikogu.ee/rito/index.php?id=14441 (18.11.2016)

[47] E. Sisas. Julgeolekusektori parlamentaarne järelevalve Eestis. Riigikogu Toimetised 2015(31). Kättesaadav: http://www.riigikogu.ee/rito/index.php?id=14441 (18.11.2016)

[48] M. Kruusamäe, T. Reinthal. Jälitustegevuse kohtulik eelkontroll Eestis: kohtupraktika analüüs. Tartu 2013, lk 29. http://www.nc.ee/?id=1252 (29.04.2016).

kasutamise ja järelevalve korraldamisel (ÕKS § 1 lg 9). Õiguskantsler on sõltumatu isik, kellel on pädevus kontrollida julgeoleku- ja luureasutuste tegevust nii luure/vastuluure, korrakaitse kui ka kriminaalmenetluse raames.

Samas on õiguskantsleri järelevalve piiratud. Näiteks ÕKS § 11^1 lg 6 ja § 37^2 lg 6 alusel ei ole õiguskantsleril ega tema asetäitja-nõunikul juurdepääsu salastatud välisteabele või riigisaladusele, mis puudutab:

1) salajasele koostööle kaasatud isikut;
2) julgeolekuasutuse tegevuse salajasel või täiesti salajasel tasemel salastatud meetodeid;
3) julgeolekuasutuse poolt teabe kogumist julgeolekuasutuste seaduse §-s 25 või 26 sätestatud viisil, kui see ei ole veel lõppenud;
4) julgeolekuasutuste rahvusvahelisi ühisoperatsioone või välisriigi või rahvusvahelise organisatsiooni poolt edastatud teavet, kui teabe edastaja ei ole juurdepääsuks nõusolekut andnud.

Lisaks eelnevale avaldab Justiitsministeerium kord aastas oma veebilehel jälitusasutustelt, prokuratuurilt ja kohtult saadud andmete alusel aruande, mis sisaldab eelmise aasta kohta järgmisi andmeid:

1) alustatud jälitustoimikute liik ja arv;
2) jälitustoimingute lubade arv jälitustoimingute liikide kaupa;
3) isikute arv, keda jälitustoimingu tegemisest teavitati ning isikute arv, kelle puhul on teavitamine vastavalt KrMS § 126^{13} lõikele 4 üle ühe aasta edasi lükatud (KrMS § 126^{15} lg 3).

Jälitustoimingute õiguspärasuse kontrollimise otstarbeks on KrMS § 126^{17} alusel loodud jälitustoimingute infosüsteem, mis on riigi infosüsteemi kuuluv andmekogu.

3.5. Julgeoleku- ja luureasutuste volitused ja meetmed elektroonilise side jälgimisel ning andmete töötlemisel ja talletamisel

3.5.1. Teabeamet

Teabeametil on teabehanke raames võimalik koguda andmeid nii elektroonilise side võrgu kaudu edastatavate sõnumite edastamise fakti, kestuse, viisi ja vormi ning edastaja või vastuvõtja isikuandmete ja asukoha andmete kohta (nn elektroonilise side meta-andmeid) (JAS § 26 lg 3 p 4) kui ka kuulata ja vaadata pealt ning salvestada elektroonilise side võrgu kaudu edastatava sõnumit või muud teavet (JAS § 25 lg 3 p 2). Samuti on võimalik siseneda varjatult arvutisüsteemi teabe varjatud kogumiseks või salvestamiseks või selleks vajalike abivahendite paigaldamiseks (JAS § 26 lg 3 p 5).

Kui elektroonilise side võrgu kaudu edastatava sõnumi või muu teabe pealtkuulamine, -vaatamine või salvestamine võib toimuda üksnes halduskohtu loal (JAS § 27 lg 1), siis elektroonilise side meta-andmete kogumise otsustab KAPO juht või tema poolt volitatud ametnik korraldusega. See korraldus kehtib selles märgitud tähtaja jooksul, kuid mitte kauem kui kaks kuud (JAS § 27 lg 3).

Ligipääs elektroonilise side andmetele, sh sõnumitele ja meta-andmetele ning sõnumi ja muu teabe pealtkuulamine toimub elektroonilise side seaduse (ESS) alusel.

Ligipääs elektroonilise side meta-andmetele toimub järelepärimisega sideettevõtjale, mis võib toimuda nii kirjalikus, elektroonilises kui ka suulises vormis (ESS § 112). Suulises vormis, kinnitades selle parooliga, võib esitada järelepärimise üksnes nn omanikupäringute kohta. Lisaks päringute esitamisele on asutustel võimalik saada ligipääs ka püsivalt (ESS § 112 lg 3 kolmas lause). Nimelt võib kirjaliku lepingu alusel tagada asutustele andmetele juurdepääsu pideva elektroonilise ühendusega. See tähendab

sisuliselt pädeva asutuse võimalust saada enda hinnangul talle vajalikke sideandmeid vahetult ilma eraldi järelepärimist esitamata.[49]

Samuti on mobiiltelefoniteenust pakkuv sideettevõtja kohustatud tagama Teabeametile mobiiltelefonivõrgus kasutatavate terminalseadmete asukoha tuvastamise reaalajas (ESS § 112 lg 3).

Jälitustoimingu teostamiseks või sõnumi saladuse õiguse piiramiseks peab sideettevõtja võimaldama jälitus- või julgeolekuasutusele juurdepääsu sidevõrgule (ESS § 113 lg 1).

Saadud teavet säilitatakse teabetoimikutes (JAS § 30), mille pidamise ja säilitamise kord on kehtestatud kaitseministri määrusega.[50] Riigisaladuseks tunnistatud teabetoimikuid säilitatakse vastavalt riigisaladuseks tunnistatud teabe säilitamise tähtajale (kaitseministri määrus § 17). Teabetoimikud, mis on lõpetatud põhjusel, et teabe kogumise alustamise ajendiks olnud esialgne teave ei ole leidnud kinnitust, hävitatakse pärast nende lõpetamist (kaitseministri määrus § 19).

3.5.2. Kaitsepolitseiamet

Vastuluures on KAPO nii JAS (§ 26 lg 3 p 4) kui ka PPVS (§ 7^{49}) alusel õigus koguda andmeid elektroonilise side võrgu kaudu edastatavate sõnumite edastamise fakti, kestuse, viisi ja vormi ning edastaja või vastuvõtja isikuandmete ja asukoha andmete kohta (nn elektroonilise side meta-andmeid). Lisaks on KAPO-l õigus kuulata ja vaadata pealt ning salvestada elektroonilise side võrgu kaudu edastatava sõnumit või muud teavet (JAS § 25 lg 3 p 2). Samuti on võimalik siseneda varjatult arvutisüsteemi teabe varjatud kogumiseks või salvestamiseks või selleks vajalike abivahendite paigaldamiseks (JAS § 26 lg 3 p 5). JAS alusel sätestatud meetmeid ning nende kasutamise protseduure on kirjeldatud eelmises alapeatükis (vt 3.5.1).

Päringu tegemine elektroonilise side ettevõtjale elektroonilise side meta-andmete saamiseks on lubatud PPVS alusel kahel viisil. Nn omanikupäringu[51] tegemiseks seadus loa taotlemise protseduuri ette ei näe. Samas muu kui omanikupäringu (andmed sõnumi edastamise fakti kohta) tegemiseks sideettevõtjale annab loa prokuratuur. Milliseid asjaolusid ja kaalutlusi peab prokuratuur loa andmiseks arvestama, seda seadus ette ei näe. Seadus näeb ette üksnes selle, et prokuratuur peab märkima kuupäevalise täpsusega ajavahemiku, mille kohta andmete nõudmine on lubatud (PPVS § 7^{49} lg 2).

Korrakaitse ülesannete täitmisel on KAPO-l õigus küsida sideettevõtjalt elektroonilise side meta-andmeid nii JAS § 26 lg 3 p 5, KorS § 35 kui ka PPVS § 7^{49} alusel. Erinevus nende meetmete kasutamisel seisneb selles, et JAS alusel toimub ligipääs nendele andmetele KAPO või tema volitatud ametniku loal, PPVS alusel toimub ligipääs muu kui omanikupäringu korral prokuratuuri loal ning KorS § 35 ei sätesta üldse loa protseduuri. Erisus seisneb ka selles, et KorS § 35 alusel tuleb isikut isikuandmete töötlemisest viivitamata teavitada ning võrreldes JAS või PPVSiga ei näe KorS ette võimalust teavitamist edasi lükata. KorS alusel võib päringu sideettevõtjale teha üksnes kirjalikult või elektrooniliselt (Kors § 35 lg 1) ning nende meetmete rakendamine tuleb igal juhul protokollida (KorS § 35 lg 2 ja 3).

KorS § 35 alusel on KAPO-l õigus saada andmeid ka mobiiltelefonivõrgus kasutatavate terminalseadmete asukoha tuvastamiseks reaalajas (KorS § 35). Korrakaitselistel eesmärkidel on lisaks võimalik siseneda varjatult arvutisüsteemi teabe varjatud kogumiseks või salvestamiseks või selleks vajalike abivahendite paigaldamiseks (JAS § 26 lg 3 p 5).

Kuriteo ettevalmistamise avastamiseks või kuriteo tõkestamise eesmärgil võib KrMS alusel vaadata või kuulata salaja pealt teavet, sh elektroonilise side võrgu kaudu edastatavat teavet (KrMS § 126^3 lg 2 p 2).

---

[49] Õiguskantsleri seisukoht: Elektroonilise side seaduse § 111^1 alusel sideandmete töötlemise põhiseaduspärasus. 22.04.2016, lk 6. Kättesaadav: http://oiguskantsler.ee/sites/default/files/field_document2/elektroonilise_side_seaduse_ss_111_1_alusel_sideandmete_tootlemise_pohiseadusparasus.pdf

[50] Kaitseministri 03.07.2001määrus nr 19 „Teabeameti teabetoimikute pidamise ja säilitamise kord“ RTL 2001, 85, 1176

[51] Elektroonilise side võrgus kasutatavate identifitseerimistunnustega seotud lõppkasutaja tuvastamiseks vajalikud andmed.

Teabe salajaseks pealtkuulamiseks või –vaatamiseks annab loa eeluurimiskohtunik (KrMS § 126^6 lg 3, § 126^7) (vt eespool punkt 3.3.2).

Kriminaalmenetluse raames võib KAPO samuti KrMS alusel vaadata või kuulata salaja pealt teavet, sh elektroonilise side võrgu kaudu edastatavat teavet (KrMS § 126^3 lg 2 p 2), milleks on vajalik eeluurimiskohtuniku luba.

Kriminaalmenetluses on võimalik ka elektroonilise side andmete nõudmine sideettevõtjalt (KrMS § 90^1). Menetlejal on õigus teha nn omaniku päringuid ilma prokuratuuri loata. Muu kui omaniku päringute puhul (st sõnumi edastamise fakti kohta) võib uurimisasutus teha üksnes prokuratuuri loal kohtueelses menetluses või kohtu loal kohtumenetluses. Päringu võib teha üksnes siis, kui see on vältimatult vajalik kriminaalmenetluse eesmärgi saavutamiseks. Päringu tegemise loas märgitakse kuupäevalise täpsusega ajavahemik, mille kohta andmete nõudmine on lubatud.

Ligipääs elektroonilise side andmetele, sh sõnumitele ja meta-andmetele ning sõnumi ja muu teabe pealtkuulamine toimub ESS alusel (vt eespool alapeatükk 3.5.1).

Elektroonilisel viisil teabe kogumisel osutab KAPO-le ametiabi korras abi Teabeamet (JAS § 7 lg 2).

3.5.3. Kaitsevägi

Kaitseväel on õigus kaitseväeluure teostamiseks koguda ja töödelda väljaspool üldkasutatavat Eesti Vabariigi territooriumil asuvat elektroonilise side võrku edastatavaid või levivaid signaale (KKS § 37 lg 1 p 1). Samuti võib Teabeamet ametiabi raames koguda Kaitseväele teavet elektroonilise side võrgu kaudu edastatava sõnumi või muud teabe pealtkuulamise, -vaatamise ning salvestamisega (KKS § 39 lg 1, JAS § 25 lg 3 p 2).

Kaitsevägi võib teha päringu elektroonilise side ettevõtjale KKS § 41^1 alusel kuriteo ettevalmistamise avastamiseks või tõkestamiseks ning tagaotsitavaks kuulutamise määruse täitmiseks. Päringu võib teha üksnes isiku suhtes, kelle puhul on põhjendatult alust arvata, et ta paneb toime kuriteo (KrMS § 126^2 lg-s 2 sätestatud kuriteo) või kes on kuulutatud tagaotsitavaks.

Sõltuvalt taotletavate andmete sisust toimub andmetele ligipääsu saamine kahel viisil. Nn omanikupäringu[52] tegemiseks seadus loa taotlemise protseduuri ette ei näe. Samas muu kui omanikupäringu (andmed sõnumi edastamise fakti kohta) tegemiseks sideettevõtjale annab loa prokuratuur. Milliseid asjaolusid ja kaalutlusi peab prokuratuur loa andmiseks arvestama, seda seadus ette ei näe. Seadus näeb ette üksnes selle, et prokuratuur peab märkima kuupäevalise täpsusega ajavahemiku, mille kohta andmete nõudmine on lubatud (KKS § 41^1 lg 2).

3.6. Järeldused läbivate üldpõhimõtete kohta julgeoleku- ja luureasutuste tegevuse reguleerimisel ning elluviimisel

Eesti julgeoleku- ja luureasutuste tegevuse regulatsiooni iseloomustab killustatus erinevate õigusaktide vahel. Kuigi julgeolekuasutuste seadus on mõlema julgeoleku- ja luureasutuse – Teabeameti ja KAPO – ja Kaitseväe jaoks üldseadus, reguleerib nende asutuste tegevust veel hulk õigusakte. Regulatsiooni killustatus esineb eelkõige KAPO puhul, sest KAPO täitab lisaks vastuluurele ka korrakaitse ja süütegude menetlemise funktsioone.

Korrakaitse ülesannete täitmisel võib KAPO lähtuda nii JAS-ist, KrMS-st, KorS-st kui ka PPVS-st. Sealjuures sätestatavad need seadused osaliselt samu meetmeid, kuigi protseduurid või põhimõtted nende kasutamiseks võivad erineda. Näiteks elektroonilise side meta-andmete päringu esitamiseks ei ole KorS alusel eelnevat loa protseduuri, samas PPVS alusel muu kui omanikupäringu korral on nõutav prokuratuuri luba (võrdluseks ka JAS alusel on vaja üksnes KAPO juhi või tema volitatud ametniku luba). Kuivõrd KAPO tegevus võib ühe eesmärgi nimel toimuda erinevatel alustel, on ebaselge, milline

[52] Elektroonilise side võrgus kasutatavate identifitseerimistunnustega seotud lõppkasutaja tuvastamiseks vajalikud andmed.

on erinevate õigusaktide – JAS, KorS, KrMS ja PPVS – koostoime ning tõusetub küsimus, mille alusel otsustab KAPO, millisest seadusest oma tegevuses lähtuda.

Samuti võib regulatsioonile ette heita ebaselgust. Näiteks ei ole piisavalt selgelt sõnastatud, millistel juhtudel Teabeameti ja KAPO JAS 4. peatükis sätestatud volitusi ning meetmeid kasutada võivad (nt JAS § 26 lg 3 puhul). Õiguskantsleri hinnangul on selle sätte muutmine vajalik, sest õigusnormide selgus ja täpsus on äärmiselt oluline põhiõiguste ja –vabaduste kaitse seisukohalt.[53] Samuti ei ole JAS-s järgitud seda põhimõtet, et kõik olulised meetmed oleksid seaduse tasemel reguleeritud. Näiteks isiku kaasamine salajasele koostööle on sätestatud siseministri määrusega (isiku kaasamine salajasele koostööle on samas seaduse tasemel reguleeritud PPVS-s). Kuivõrd Teabeameti meetodite ja vahendite vastav ministri määrus on salastatud, ei ole võimalik teha järeldusi selle kohta, kas Teabeameti puhul on kõik meetodid seaduse tasemel reguleeritud.

Seda, et julgeolekuasutuste kriminaalmenetluse väline jälitustegevuse õiguslik raamistik on üldsõnaline, piiritlemata ja süstematiseerimata ning et olemasolev regulatsioon vajaks tervikuna ümbervaatamist, on kinnitatud nii õiguskantsleri arvamuses[54] kui ka Riigikohtu analüüsis[55].

Eesti regulatsioon sätestab erinevad meetmed ning protseduurid (*ex ante* kui ka *ex post* järelevalve protseduurid) nende meetmete kasutamisel põhiõiguste riive õiguspärasuse tagamiseks. Regulatsioonist nähtub, et julgeoleku tagamisel ning muude julgeolekuasutuste ülesannete täitmisel on lubatud kasutada erinevaid meetmeid, mis piiravad isikute põhiõigusi.

Julgeolekukontrolli tegemisel on asutustel väga laiaulatuslikud volitused, sest lubatud on jälitustoimingute tegemine. Samas ei ole selge, kui kaugele täpselt võib julgeolekukontrolliga minna ning kas selline intensiivne riive on tõepoolest õigustatud. Samuti on probleemne küsimus, kas näiteks advokaadi julgeolekukontrollile allutamine peaks olema lubatud või mitte.[56]

Põhiõigusi riivavate meetmete kõrval nähakse ette mitmed üldpõhimõtted, nt proportsionaalsuse põhimõte, *ultima ratio* põhimõte, ja tagatised, et isikute põhiõiguseid ei riivataks rohkem kui vajalik. Lisaks näeb regulatsioon ette eelneva sõltumatu kohtuliku kontrolli sõnumi saladust rikkuva või väga tõsise kodu, perekonna- või eraelu puutumatuse rikkumise korral (varjatud sisenemine ruumi, hoonesse, arvutisüsteemi jne). Enamuse meetmete kasutamine toimub siiski kas prokuratuuri või asutuse juhi loal. Euroopa Inimõiguste Kohtu hinnangul ei saa ülehinnata kohtuliku kontrolli väärtust võttes arvesse, millistes tohututes kogustes on ametiasutustel võimalik saada informatsiooni ning seda töödelda peaaegu kõigi isikute kohta.[57] Euroopa Inimõiguste Kohus on samas märkinud, et eelnev (*ex ante*) volituse andmine ei ole ilmtingimata vajalik, kui on olemas tugev kohtulik järelkontroll, mis võib tasakaalustada algse volituse andmise puudujääke.[58]

Käesoleval juhul ei saa prokuratuuri kontrolli pidada piisavaks seetõttu, et kohtulik järelkontroll on tagatud üksnes nende juhtudel, kui näiteks kriminaalmenetlus jõuab süüdistuseni, milles esitatakse vastavate meetmetega kogutud tõendid. Kõik kriminaalmenetlused, milles jälitustoiminguid tehakse, samuti kriminaalmenetluse väline jälitustegevus, ei jõua alati kohtusse.[59] Riigikohus on olnud seisukohal, et olukorras, kus isik ei ole oma põhiõigusi riivavast jälitustoimingust teadlik, on praktiliselt välistatud võimalus kasutada põhiõigust pöörduda oma õiguste kaitseks kohtu poole.[60] Arvesse tuleb võtta samas seda, et kehtiv regulatsioon lubab jätta isiku teavitamata (või seda vähemasti edasi lükata)

---

[53] Õiguskantsler. (2015). Arvamus julgeolekuasutuste seaduse ning politsei ja piirivalve seaduse muutmise seaduse eelnõu väljatöötamise kavatsusele. Kättesaadav aadressilt http://oiguskantsler.ee/sites/default/files/field_document2/6iguskantsleri_arvamus__julgeolekuasutuste_seaduse_ning_politsei_ja_piirivalve_seaduse_muutmise_seaduse_eelnou_valjatootamise_kavatsus.pdf lk 2.

[54] *Ibid*.

[55] A. Lott. Põhiseadusliku korra kaitseks teostatav jälitustegevus Eestis. Riigikohus: Tartu 2015. – http://www.riigikohus.ee/vfs/1906/PKK%20j%E4litustegevuse%20anal%FC%FCs.pdf

[56] http://www.postimees.ee/316505/advokatuur-kaitsja-ei-pea-julgeolekukontrolliga-noustuma , http://www.aripaev.ee/uudised/2016/08/02/riigisaladuse-loaga-advokaat-on-haruldus

[57] EIKo, 12.01.2016, 37138/14, *Szab and Vissy vs Hungary*, p 79.

[58] EIKo, 12.01.2016, 37138/14, *Szab and Vissy vs Hungary* p 77; EIKo 18.05.2010, 26839/05, *Kennedy*, p 167.

[59] RKPSJKo 3-4-1-42-13, p 49.

[60] RKPSJKo 3-4-1-42-13, p 49.

tema suhtes võetud meetmetest, kui see ohustab mingil viisil uurimist. Sellisel juhul ei ole aga isikul võimalik oma õiguste rikkumisest teada saada ning oma õigusi efektiivselt kaitsta.

Ühe *ex post* järelevalve protseduuri riigikogu julgeolekuasutuste järelevalve komisjoni töö osas on avaldatud kahtlust, kas sellel komisjonil on piisavalt pädevust ning ressursse tõhusaks kontrolliks.[61] Samuti on ette heidetud seda, et tegelikkuses sõltub järelevalve erikomisjoni tegelik töö sisu ja ulatus liikmete tahtest ja tõlgendustest ning komisjoni käsutuses olevad ressursid ei toeta efektiivset parlamentaarset järelevalvet julgeolekuasutuste üle.[62] Samuti on piiratud õiguskantsleri kontroll, sest õiguskantsleril ega tema asetäitjatel ei ole juurdepääsu salastatud välisteabe või riigisaladusele, mis puudutab näiteks julgeolekuasutuste tegevuse salajasel või täiesti salajasel tasemel salastatud meetodeid, samuti julgeolekuasutuste poolt teabe kogumist JAS-s sätestatud meetmetega, kui see tegevus ei ole veel lõppenud.

Kokkuvõtlikult lähtub olemasolev regulatsioon põhimõttest, et julgeoleku kaalutlustel võib isikute põhiõiguseid riivata. Teiselt poolt näeb regulatsioon ette mitmed üldpõhimõtted, nt proportsionaalsuse põhimõtte, ning erinevad kontrollimehhanismid (tagatised), et isikute põhiõiguseid ei riivataks rohkem kui vajalik. Samas ei ole üheselt selge, kuivõrd tegelikkuses suudavad olemasolevad *ex ante* ja *ex post* järelevalve protseduurid põhiõiguste riive õiguspärasust tagada.

[61] U. Lõhmus. Pealtkuulamine ja Eesti põhiseaduses sätestatud õigus sõnumite saladusele. – Juridica 2008/VII, lk 472. E. Sisas. Julgeolekusektori parlamentaarne järelevalve Eestis. Riigikogu Toimetised 2015(31). Kättesaadav: http://www.riigikogu.ee/rito/index.php?id=14441 (18.11.2016)
[62] Ibid.

4. ROOTSI

4.1. Julgeoleku- ja luureasutused ning nende tegevust reguleerivad õigusaktid

Rootsi julgeoleku- ja luureasutused jagunevad kahte gruppi:

1) **Kaitsepolitsei** (*Säkerhetspolisen, SÄPO*), mis tegeleb julgeolekualaste kuritegude vastase võitlusega;
2) **Kaitsejõud** (*Försvarsmakten*)[63], **Raadioluureamet** (*Försvarets Radioanstalt, FRA*), **Kaitsejõudude Relvastuse ja Kaitsetehnika Amet** (*Försvarets materielverk, FMV*) ja **Totaalkaitse Uurimisinstituut** (*Totalförsvarets forskningsinstitut, FOI*), mis tegelevad välisluurega.

Kaitsepolitsei tegevust puudutavad järgnevad õigusaktid:

1) Politseiseaduses (*Polislag* (1984:387), edaspidi: *PL*) on reguleeritud Kaitsepolitsei ülesanded, volitused ja kohustused;
2) Seaduses andmetöötlusest politseis (*Polisdatalag* (2010:361), edaspidi: *PDL*) on reguleeritud politsei (sh Kaitsepolitsei) volitused isikuandmete töötlemisel ja isikuandmete töötlemise nõuded;
3) Määruses „Juhend Kaitsepolitsei jaoks“ (*Förordning* (2014:1103) *med instruktion för Säkerhetspolisen*, edaspidi: *FMIS*) on reguleeritud Kaitsepolitsei vastutusvaldkonnad ja valitsusele aru andmise kord;
4) Seadus teatud ühiskonnaohtlike kuritegude väljaselgitamise meetmete kohta (*Lag* (2008:854) *om åtgärder för att utreda vissa samhällsfarliga brott*, edaspidi: *LSB*) sätestab julgeolekualaste kuritegude väljaselgitamise meetmed ja nende rakendamise korra;
5) Seadus teatud eriti ohtlike kuritegude ennetamise meetmete kohta (*Lag* (2007:979) *om åtgärder för att förhindra vissa särskilt allvarliga brott*, edaspidi: *LSAB*) sätestab julgeolekualaste kuritegude ennetamise meetmed ja nende rakendamise korra;
6) Kriminaalmenetluse seadustikus (*Rättegångsbalk* (1942:740) edaspidi: *RGB*) on reguleeritud julgeolekualaste kuritegude uurimisel kasutatavad meetmed;
7) Seadus teatud kuritegevuse vastase tegevuse järelevalve kohta (*Lag* (2007:980) *om tillsyn över viss brottsbekämpande verksamhet*, edaspidi: *LBV*) reguleerib Julgeoleku ja Isikuandmete Kaitse Komisjoni tegevust;
8) Julgeolekukaitse seadus (*Säkerhetsskyddslag* (1996:627), edaspidi: *SL*) reguleerib julgeolekukontrolli tegemist;
9) Seadus, mis käsitleb elektroonilise side andmete kogumist õiguskaitseasutuste uurimistegevuse raames (*Lag* (2012:278) *om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet*, edaspidi: *LBMU*);
10) Elektroonilise side seadus (*Lag* (2003:389) *om elektronisk kommunikation*, edaspidi: *LEK*).

Välisluurealast tegevust puudutavad järgnevad õigusaktid:

1) Välisluurealase tegevuse seadus (*Lag* (2000:130) *om försvarsunderrättelseverksamhet*, edaspidi: *LF*) sätestab välisluure teostamise eesmärgid ja reguleerib välisluureinfo jagamist teiste riikide ja organisatsioonidega. Seadust täpsustab välisluure alase tegevuse määrus (*Förordning* (2000:131) *om försvarsunderrättelseverksamhet*, edaspidi: *FFV*), milles on mh määratletud välisluuret teostavad organid;
2) Seaduses isikuandmete töötlemise kohta Rootsi Kaitsejõudude välisluuretegevuses ja sõjaväelises julgeolekuteenistuses (*Lag* (2007:258) *om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst*, edaspidi: *LMS*) on reguleeritud luuretegevuse käigus isikuandmete töötlemine Rootsi Kaitsejõudude poolt;
3) Raadioluureameti tegevust puudutavad õigusaktid:

[63] Kaitsejõududes tegeleb välisluurega Militära underrättelse- och säkerhetstjänsten (MUST, Military Intelligence and Security Service)

a. Seaduses välisluurealase tegevuse raames teostatava signaalluure (kommunikatsiooniluure) kohta (*Lag* (2008:717) *om signalspaning i försvarsunderrättelseverksamhet*, edaspidi: *LSF*) on reguleeritud signaalluure teostamise alused, kord ja järelevalve;
b. Seaduses isikuandmete töötlemise kohta Raadioluureameti välisluure- ja arendustegevuses (*Lag* (2007:259) *om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet*, edaspidi: *LFRF*) on reguleeritud Raadioluureameti volitused isikuandmete töötlemisel, järelevalve isikuandmete töötlemise üle ja isikuandmete töötlemise nõuded;
c. Määruses „Juhend Raadioluureameti jaoks" (*Förordning* (2007:937) *med instruktion för Försvarets radioanstalt*, edaspidi: *FFR*) on reguleeritud Raadioluureameti ülesanded ja ülesehitus;
d. Seadus Kaitseteabekohtu kohta (*Lag* (2009:966) *om Försvarsunderrättelsedomstol*, edaspidi *LFR*) reguleerib Kaitseteabekohtu tegevust. Seadust täpsustab määrus „Juhised Kaitseteabekohtule" (*Förordning* (2009:968) *med instruktion för Försvarsunderrättelsedomstolen*);
e. Määrus „Juhised Riiklikule Kaitseteabe Inspektsioonile" (*Förordning* (2009:969) *med instruktion för Statens inspektion för försvarsunderrättelseverksamheten*, edaspidi: *FSIF*) reguleerib Kaitseteabe Inspektsiooni tegevust.

Kaitsepolitsei ja välisluureasutuste tegevust puudutavad lisaks järgnevad õigusaktid:

1) Kvalifitseeritud kaitseidentiteetide seadus (*Lag* (2006:939) *om kvalificerade skyddsidentiteter*, edaspidi: *LKS*), mis sätestab luure- või uurimistegevuses osalevatele isikutele kvalifitseeritud kaitseidentiteedi andmise alused ja korra;
2) Riksdagi seadus (*Riksdagsordning* (2014:801), edaspidi: *RO*) reguleerib parlamendikomisjonide tööd;
3) Seadus juhistega parlamentaarsele ombudsmanile (*Lag* (1986:765*) med instruktion för Riksdagens ombudsmän*, edaspidi: *LRO*) reguleerib parlamentaarse ombudsmani poolt haldusorganite üle teostatavat järelevalvet.

4.2. Julgeoleku- ja luureasutuste ülesanded, volitused ja meetmed põhiõiguste piiramisel

Kaitsepolitsei (*Säkerhetspolisen*, SÄPO) tegeleb FMIS § 1 kohaselt julgeolekuteenistusena teabe hankimise ja julgeolekutööga. Alates 2015. aastast on Kaitsepolitseiamet iseseisev asutus, mis ei kuulu ülejäänud politsei koosseisu. Sellist lahutamist peetakse üldiselt eelistatavaks, kuna see väldib salajaselt kogutud teabe meelevaldset kasutamist.[64]

Kaitsepolitsei põhiülesanded on järgmised (PL § 3):

1) riigi julgeoleku vastu suunatud kuritegeliku tegevuse või terrorismi ennetamine, takistamine ja avastamine ning nende kuritegude uurimine ja vajalike meetmete rakendamine;
2) ülesannete täitmine seoses riigijuhtide ja muude valitsuse või julgeolekupolitsei poolt määratud isikute ihukaitsega;
3) SL-st tulenevate teiste ülesannete täitmine ehk julgeolekukontrollide läbi viimine ja riigiasutuste kasutuses oleva konfidentsiaalse teabe kaitsmine;
4) muu politseilise tegevuse teostamine.

PL § 1 kohaselt teevad politseitööd politseiasutus ja Kaitsepolitsei.

[64] European Union Agency for Fundamental Rights. Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU, 2015: http://fra.europa.eu/sites/default/files/fra_uploads/fra-2016-surveillance-intelligence-services_en.pdf, lk 14.

Välisluurealast tegevust teostavad **Kaitsejõud** (*Försvarsmakten*), **Raadioluureamet** (*Försvarets Radioanstalt*, FRA), **Kaitsejõudude Relvastuse ja Kaitsetehnika Amet** (*Försvarets materielverk,* FMV) ja **Totaalkaitse Uurimisinstituut** (*Totalförsvarets forskningsinstitut*, FOI) (FFV § 2).

Välisluurealase tegevuse eesmärgiks on toetada Rootsi välis-, julgeoleku- ja kaitsepoliitikat ning kaardistada muid riigi vastu suunatud välisohtusid (LF § 1). Sama sätte kohaselt võib välisluurealane tegevus puudutada üksnes välisküsimusi.

4.2.1. Kaitsepolitsei volitused ja meetmed

Kaitsepolitsei meetmed julgeolekualaste kuritegude ennetamiseks on järgmised:

1) elektroonilise side salajane pealtkuulamine ja jälgimine (LSAB §-d 1 ja 2);
2) juurdepääs elektroonilise side andmetele (LBMU §-d 2 ja 3);
3) salajane videovalve (LSAB §-d 1 ja 3);
4) kirjade, postipakkide ja telegrammide ja muude postiasutuses olevate saadetiste uurimine, avamine ja läbivaatamine (LSAB § 4).

Kaitsepolitsei meetmed julgeolekualaste kuritegude uurimiseks kriminaalmenetluse käigus on:

1) elektroonilise side salajane pealtkuulamine ja jälgimine (LSB § 3);
2) juurdepääs elektroonilise side andmetele (LEK 6. ptk, § 22, RGB 27. ptk, § 19);
3) salajane videovalve (LSB § 3);
4) saadetiste konfiskeerimine (LSB § 2).

Kriminaalmenetluse seadustikus (RGB) on julgeolekualaste kuritegude uurimiseks täiendavalt ette nähtud tehniliste vahendite abil heli salajase pealtkuulamise kasutamine (ingl k *bugging*) (RGB 27. ptk §-d 20d–20e, § 25a). Samas seaduses on üldise meetmetena (mitte ainult julgeolekualaste kuritegude uurimiseks) ette nähtud isiku vahistamine (RGB 24. ptk), hoone, ruumi või kinnise ala läbiotsimine (RGB 28. ptk §-des 1-10), isiku läbiotsimine (RGB 28. ptk § 11) ja isiku füüsiline läbivaatus ja proovide võtmine (RGB 28. ptk § 12).

Politseilise tegevuse teostamisel on Kaitsepolitsei ametnikel õigus kasutada ka samu meetmeid, mis politseiametnikel üldiselt (PL § 3 p-i 5) ehk seaduses sätestatud tingimustel on lubatud:

1) jõu (vägivalla) kasutamine (PL § 10);
2) käeraudade kasutamine (PL § 10a);
3) ajutine vahistamine (PL § 11);
4) isiku alalt või ruumist ära saatmine (PL § 13 – § 13c);
5) vahistamine isiku kindlakstegemise eesmärgil (PL § 14);
6) isiku läbiotsimine (PL § 19);
7) majja, ruumi või kohta sisenemine (PL § 20, 21, 23) ja ligipääsu keelamine või muude sarnaste meetmete rakendamine (PL § 23 p 2, § 24);
8) sõiduki peatamine (PL § 22) ja läbiotsimine (PL § 20 a);
9) rahvakogunemisel osalejatele korralduse andmine kindlas suunas liikumiseks (§ 24);

Kaitsepolitseile on antud ulatuslikud volitused isikuandmete töötlemiseks (PDL). Kaitsepolitsei tohib isikuandmeid töödelda mh siis, kui see on vajalik julgeolekualaste kuritegude ära hoidmiseks, tõkestamiseks ja avastamiseks (PDL § 1 p 1) või rahvusvahelistest kohustustest tulenevate ülesannete täitmiseks (PDL § 1 p 5). Kaitsepolitsei võib isikuandmeid töödelda ka teistele asutustele, sh Kaitsejõududele info andmiseks (PDL § 2).

Kaitsepolitseis töötavatele isikutele on ette nähtud kaitseidentiteedi kasutamise võimalus (LKS). LKS § 1 ja 4 kohaselt kantakse kaitseidentiteedi määramisel isikut tuvastavatesse dokumentidesse ja riiklikesse registritesse isiku tegelike isikuandmete asemel kaitseidentiteet.

Julgeolekukontrolli läbiviimiseks on Kaitsepolitseil õigus töödelda riigi andmekogudes olevaid andmeid ning avalikkuses kättesaadavaid andmeid (SL §-d 13–18).

4.2.2. Välisluurega tegelevate asutuste volitused ja meetmed

Välisluurega tegelevad asutustel on oma ülesannete täitmiseks õigus hankida informatsiooni, seda töödelda ning analüüsida (LF). Sealjuures kasutatakse oma ülesannete täitmisel tehnilist ja isikupõhist informatsiooni hankimist (LF § 2).

Informatsiooni tehnilise hankimise meetmed on täpsemalt reguleeritud signaalluure puhul. Muid välisluure teostamise meetmeid õigusaktides täpsemalt reguleeritud ei ole.

Elektroonilise side jälgimise ehk signaalluurega tegeleb Rootsis **Raadioluureamet** (*Försvarets Radioanstalt,* FRA) (FFR § 1).

Järgnevalt käsitletakse Raadioluureameti poolt teostatavat üldist elektroonilise side jälgimist ehk signaalluuret, st otsingusõnadel põhinevat üldist jälgimist, mis ei ole suunatud konkreetsete isikute jälgimisele (ingl k *mass surveillance)*. Signaalluure teostamise kord on LSF-s.

LSF § 1 kohaselt võib Raadioluureamet koguda signaalluure käigus elektroonilises vormis signaale. Sättes on ka loetletud julgeolekuohud, mille kaardistamise eesmärgil signaalluuret teostada võib ning nendeks on:

1) väljastpoolt lähtuvad riigi vastu suunatud ohud;
2) eeldused Rootsi osalemiseks rahvusvahelistes rahutagamis- ja humanitaaroperatsioonides või selliste operatsioonide käigus Rootsi huvide julgeolekut ähvardavad ohud;
3) strateegilised asjaolud, mis on seotud rahvusvahelise terrorismi ja muu raske rahvusvahelise kuritegevusega, mis võib ohustada olulisi rahvuslikke huvisid;
4) massihävitusrelvade, sõjavarustuse ja kahesuguse kasutusega toodete areng ja levik;
5) tõsised väljastpoolt lähtuvad ühiskonna infrastruktuuride vastu suunatud ohud;
6) välismaal asetleidvad konfliktid, mis võivad mõjutada rahvusvahelist julgeolekut;
7) Rootsi huvide vastu suunatud võõra päritoluga luuretegevus;
8) Rootsi välis-, julgeoleku- või kaitsepoliitika seisukohalt oluline võõraste võimude tegutsemine ja kavatsused.

Kui see on välisluurealase tegevuse seisukohalt vajalik, võib elektroonilises vormis signaalide hankimine signaalluure käigus LSF § 1 kohaselt toimuda ka eesmärgiga:

1) jälgida ümbritsevas signaalkeskkonnas, tehnika arengu valdkonnas ja signaalkaitse toimuvaid muutusi ja
2) arendada jooksvalt tehnikat ja metoodikat, mis on vajalik käesoleva seaduse kohase tegevuse teostamiseks.

Raadioluureamet ei teosta signaalluuret omal algatusel. Signaalluure suuna määravad valitsus, Kaitsejõud, Kaitsepolitsei ja Politseiameti rahvusliku tähtsusega küsimustega tegelev operatiivosakond (LSF §-d 1, 4). Signaalluure võib puudutada ainult signaale, mida edastatakse üle Rootsi piiride ning keelatud on koguda signaale, mille edastaja ja vastuvõtja asuvad mõlemad Rootsis (LSF §-d 2 – 2a).

LSF § 3 sätestab signaalluure teostamise tehnilise korra. Sätte kohaselt toimub signaalluure automatiseeritult ning võib puudutada ainult otsinguterminite abil identifitseeritud signaale.

Raadioluureameti tegevuses reguleerib isikuandmete töötlemist LFRF, mille § 8 annab Raadioluureametile üldise volituse isikuandmete töötlemiseks: isikuandmete töötlemine on lubatud, kui isik on seotud välisluuretegevuse täpsustatud suunaga ja isikuandmete töötlemine on vajalik selle suuna järgmiseks.

Välisluurealase tegevuse seadust (LF) täpsustab FFV. Selle kohaselt võivad välisluurega tegelevad asutused teha luurealastes küsimustes koostööd teiste riikide ja rahvusvaheliste organisatsioonidega

eeldusel, et koostöö eesmärgiks on tegutsemine Rootsi riigi huvides (FFV § 3) ning koostööst informeeritakse Kaitseministeeriumi (FFV § 4).

Isikuandmete töötlemine välisluuretegevuses on reguleeritud LMS-s. LMS kohaldub juhul, kui töötlemine on täies mahus või osaliselt automatiseeritud või kui andmed kuuluvad või on ette nähtud kuuluma isikuandmete struktureeritud kogusse (LMS § 1). LMS-s on sätestatud üldine volitus isikuandmete töötlemiseks: Rootsi Kaitsejõud võivad oma välisluuretegevuse ja sõjaväelise julgeolekuteenistuse käigus töödelda seaduses ära toodud eeldustel andmekogudes sisalduvaid isikuandmeid (LMS § 7). Isikuandmete töötlemiseks peab siiski olema põhjendatud alus konkreetse isiku kontrollimiseks, nt kui on põhjendatud alus eeldada, et isik on toime pannud või võib toime panna riigi julgeolekut ohustava kuriteo või terroriakti (LMS § 10).

Välisluurega tegelevates asutustes töötavatele isikutele on ette nähtud kaitseidentiteedi kasutamise võimalus (LKS). LKS § 1 ja 4 kohaselt kantakse kaitseidentiteedi määramisel isikut tuvastavatesse dokumentidesse ja riiklikesse registritesse isiku tegelike isikuandmete asemel kaitseidentiteet.

4.3. Protseduurid põhiõiguste riive õiguspärasuse tagamiseks

4.3.1. Protseduurid Kaitsepolitsei tegevuse õiguspärasuse tagamiseks

Järgnevalt käsitletakse spetsiaalselt julgeolekukuritegude ennetamiseks ja uurimiseks ette nähtud jälitusmeetmeid ja seejärel meetmeid, mida on õigus kasutada politseinikel üldiselt.

(a) Protseduurid spetsiaalselt julgeolekukuritegude ennetamiseks ja uurimiseks ette nähtud jälitusmeetmetele

LSB-s (§ 1) ja LSAB-s (§ 1) on loetletud julgeolekualased kuriteod, mille ennetamiseks või uurimiseks on lubatud elektroonilise side salajane pealtkuulamine ja jälgimine, salajane videovalve, saadetiste uurimine ja konfiskeerimine (nt sabotaaž, riigireetmine, sõjaõhutamine, terrorismialased kuriteod, mäss, relvastatud ähvardus seadusliku korra vastu).

Julgeolekualaste kuritegude uurimiseks (mitte ennetamiseks) on lubatud ka tehniliste vahendite abil heli salajane pealtkuulamine (ingl k *bugging*, RGB ptk 27 § 20d). Nimetatud meetmete kasutamiseks on vajalik kohtu luba (LSAB § 6, LSB § 3, RGB ptk 27 § 21). Loa andmise menetluses osaleb jurist, kes esindab isikute huvi eraelu puutumatusele (RGB ptk 27 § 26). Juhul, kui kohtu loa saamine tooks kaasa viivituse, mis takistab kuriteo ärahoidmist või takistab oluliselt uurimist, võib loa anda ka prokurör (LSAB § 6a, LSB § 4 ja 5, RGB ptk 27 § 21a). Kohus vaatab prokuröri antud loa kiiremas korras üle ning võib selle tühistada, kui alus meetme rakendamiseks puudus (LSAB § 6a, LSB § 6, RGB ptk 27 § 21a). Prokurör ei saa anda luba tehniliste vahendite abil heli salajaseks pealtkuulamiseks, selleks on igal juhul vaja kohtu luba (RGB ptk 27 § 21a).

Kuriteo ennetamise eesmärgil tohib meetme kasutamise loa anda ainult juhul, kui meetmel on kuriteo takistamisel eriline kaal ja meetme kasutamise põhjendus kaalub üldiselt üles sekkumise või kahju, mille meede uuritavale isikutele põhjustab (LSAB § 5). Kui meetmete kasutamiseks ei ole enam alust, tühistab prokurör või kohus loa viivitamatult (RGB ptk 27 § 23).

RGB (ptk 27 § 31) näeb ette üldise reegli, et isikut teavitatakse tema suhtes kasutatud jälitusmeetmetest. See reegel ei kehti aga julgeolekualaste kuritegude puhul (RGB ptk 27 § 33).

Elektroonilise side salajane pealtkuulamine ja jälgimine ennetuseesmärgil hõlmab ainult selle isiku telefoninumbrit või elektroonilist sidevahendit, kelle suhtes on alust arvata, et ta paneb kuriteo toime ja telefoninumbrit või elektroonilist sidevahendit, mille suhtes on eriline põhjus arvata, et eelpool nimetatud isik nendega ühendust võtab (LSAB § 2, RGB ptk 27 § 20).

Salajane videovalve ennetuseesmärgil hõlmab ainult kohta, kus isik, kelle suhtes on alust arvata, et ta kuriteo toime paneb, võib arvatavalt viibida või kohta, kus kuritegelik tegevus võib toimuda ja selle lähiümbrust (LSAB § 3, RGB ptk 27 §-d 20b, 20c).

Saadetise konfiskeerimisest teavitatakse saatjat ja adressaati nii kiiresti, kui see on ilma uurimise takistamiseta võimalik (RGB ptk 27 § 11).

Salajane pealtkuulamine on lubatud ainult kuriteos kahtlustatava isiku tavapärases viibimiskohas või kohas, mille suhtes on konkreetne alus arvata, et kuriteos kahtlustatav isik seal viibib. Salajane pealtuulamine ei ole lubatud kohtades, mida kasutatakse püsivalt ajakirjanike poolt kelle suhtes kehtib allikakaitse või arstide, advokaatide või teiste kutsesaladuse hoidmise kohustusega hõlmatud isikute poolt ning püsivalt usutegevuseks kasutatavates kohtades (RGB ptk 27 § 20e).

Kaitsepolitseile on salajaseks pealtkuulamiseks või salajaseks videovalveks lubatud anda ka luba salaja siseneda kohta, mis üldiselt on kaitstud, et sinna jälgimisseadmeid paigutada. Sel viisil ei või siiski jälgimisseadmeid paigutada isiku koju (RGB ptk 27 § 25a).

Juurdepääs elektroonilise side andmetele on lubatud üksnes selliste kuritegude ärahoidmiseks, ennetamiseks või avastamiseks, mille eest on karistuseks ette nähtud vähemalt kaheaastane vangistus või mis on loetletud LBMU §-s 3. Juurdepääsu elektroonilise side andmetele otsustab asutuse juht või selleks volitatud töötaja ning see meede ei tohi kesta kauem kui üks kuu (LBMU § 5). Igast andmete kogumise otsusest tuleb teavitada Julgeoleku ja Isikuandmete Kaitse Komisjoni (LBMU § 6).

Kuritegude uurimiseks on juurdepääs elektroonilise side andmetele lubatud kuritegude puhul, mille eest on karistusena ette nähtud vähemalt kuuekuuline vangistus (RGB 27. ptk § 19). Selleks peab prokuratuur taotlema loa pädevalt kohtult, välja arvatud kiireloomulise juhtumi korral (RGB 27. ptk §-d 19 ja 21).

(b) Protseduurid politseiametnike üldistele meetmetele

RGB 24. ptk-s on reguleeritud isiku vahistamine kriminaalmenetluse käigus (24. ptk-i §-des 1 ja 2). Isiku võib vahistada, kui teda kahtlustatakse kuritegudes, mille eest saab karistada vähemalt aasta pikkuse vangistusega ning kui tema vabadusse jäämine oleks ohtlik, samuti kui ta varjab oma isikut. Isiku vahistamine on lubatud politseiniku, politseiasutuse või kohtu otsuse alusel, sealjuures politsei ja prokuröri otsuse alusel vastavalt kuni 12 tunniks või kolmeks päevaks (RGB 24. ptk §-d 7, 8 ja 12, 23. ptk § 9).

RGB 28. ptk §-des 1–10 on reguleeritud hoone, ruumi või kinnise ala läbiotsimine. Meetme kasutamine on lubatud kohtu või prokuröri loal (RGB § 4). Kui on viivituse oht, võib läbiotsimise läbi viia ka politseinik oma otsuse alusel (RGB § 5).

RGB 28. ptk §-des 11–13 on reguleeritud isiku läbiotsimine ning isiku füüsiline läbivaatus ja proovide võtmine. Isiku läbiotsimine on lubatud, kui on alust uskuda, et läbiotsimisel võib leida tõendeid või kuriteoga saadud vara. Isiku läbiotsimist, füüsilist läbivaatust ja proovide võtmist tuleb läbi viia privaatses ruumis, proovide võtmine on lubatud ainult meditsiinitöötaja poolt.

Politseiseaduses on sätestatud eelkõige korrakaitselise iseloomuga meetmed. Seetõttu on nende kasutamise eelduseks üldjuhul mingi avaliku korra rikkumise või selle ohu esinemine. Iga meetme puhul on täpsustatud, mis tüüpi avaliku korra rikkumine või oht meetme kasutamiseks esinema peab. Nii on näiteks majja, ruumi või kohta sisenemine lubatud siis, kui võib eeldada, et mingis kohas on tegemist kuriteo sooritamise ohuga, millega kaasneb tõsine oht inimeste elule või tervisele või vara ulatuslikku hävitamise oht (PL § 23). Jõu kasutamine on ette nähtud *ultima ratio* meetmena, st jõu kasutamine on lubatud ainult juhul, kui teised meetmed on ebapiisavad (PL § 10).

4.3.2. Protseduurid välisluurega tegelevate asutuste tegevuse õiguspärasuse tagamiseks

Välisluurealase suuna sätestab valitsus (LF § 1). Seega ei ole välisluurega tegelevatel asutustel õigust välisluuret teostada enda määratud eesmärkidel, vaid nad peavad lähtuma valitsuse antud suunistest.

Täpsed protseduurid välisluurealase tegevuse õiguspärasuse tagamiseks on ette nähtud Raadioluureameti poolt teostatava elektroonilise side jälgimiseks. Ülejäänud välisluure osas ei näe seadus ette spetsiifilisi protseduure välisluure alase tegevuse õiguspärasuse tagamiseks, v.a. *ex post* järelevalve, mida on käsitletud järgnevas alapeatükis.

Välisluurealase tegevuse raames ei tohi rakendada meetmeid, mille eesmärgiks on ülesannete lahendamine, mis seaduste ja teiste ettekirjutuste kohaselt kuuluvad Politseiameti, Kaitsepolitsei ja teiste

kuriteovastase võitluse või kuritegude ennetamisega tegelevate ametkondade pädevusalasse (LF § 4). Seeläbi välditakse välisluurega tegelevatele asutustele liiga laiaulatuslike volituste andmist.

Signaalluureseaduse üldpõhimõtteks on, et üldjuhul ei tohi signaalluure puudutada ühte isikut, vaid tegemist on üldise luurega. Nii ei tohi valitsuse või teiste asutuste määratud signaalluure suund puudutada üksnes ühte füüsilist isikut (LSF § 4) ning ka kindla isikuga seostatavaid otsingutermineid võib kasutada ainult juhul, kui see on äärmiselt tähtis (LSF § 3). Raadioluureametil on kohustus isikut teavitada, kui signaalluure käigus on kasutatud otsingutermineid, mis seonduvad konkreetse isikuga (LSF § 11a). Teavitamiskohustus ei ole siiski juhul, kui teabe edastamist takistab selle salastatus või kui informatsioon puudutab ainult suhteid võõrriikide vahel (LSF § 11b). 2015. aasta seisuga ei olnud ühtegi teavitust eeltoodud sätete alusel tehtud.[65]

Otsinguterminid töötatakse välja ja neid kasutatakse lugupidamisega üksikisiku puutumatuse suhtes ja viisil, et signaalluurega kaasnev isikupuutumatuse rikkumine oleks maksimaalselt piiratud ulatusega (LSF § 3).

Juhul, kui kogutakse informatsiooni, mis puudutavad konkreetset füüsilist isikut ning mis ei ole julgeolekuohtude kaardistamiseks olulised, on Raadioluureametil kohustus kogutud informatsioon hävitada (LSF § 7 p 1). Informatsiooni hävitamise kohustus on Raadioluureametil ka juhul, kui informatsioon on kaitstud ajakirjandusliku allikakaitsega või sisaldab kaitsja ja süüdistatava suhtlust ning kui informatsioon sisaldab pihi või hingehoiu käigus antud informatsiooni ja ei ole oluline julgeolekuohtude kaardistamiseks (LSF § 7 p-d 2 – 4).

Raadioluureamet võib signaalluuret läbi viia ainult juhul, kui selleks on loa andnud Kaitseteabekohus (*Försvarsunderrättelsedomstolen*) (LSF § 4a). Seega teostab Kaitseteabekohus Raadioluureameti tegevuse üle *ex ante* järelevalvet. Erandjuhtudel, kui Kaitseteabekohtult loa saamine tooks kaasa viivituse või muu takistuse, mis takistaks signaalluure eesmärkide saavutamist, võib loa anda ka valitsuse määratud Raadioluureameti ametnik. Sel juhul tuleb Kaitseteabekohut loast viivitamata teavitada ning Kaitseteabekohtul on võimalik luba tühistada või muuta (LSF § 5b).

Kaitseteabekohus annab LSF § 5 alusel loa signaalluure teostamiseks, kui:

1) ülesanne on kooskõlas välisluuret ja signaalluuret reguleerivate seadustega;
2) informatsiooni hankimise eesmärki ei ole võimalik täita vähema sekkumisega;
3) ülesande täitmise tulemusel saadakse eelduslikult informatsiooni, mille väärtus on selgelt kõrgem kui puutumatuse rikkumine, mida taotluse alusel teostatav info hankimine võib endas sisaldada;
4) kasutamiseks kavandatud otsingumõisted või nende kategooriad on kooskõlas LSF §-ga 3;
5) taotlus ei puuduta üksnes ühte füüsilist isikut.

Kaitseteabekohtu antud loas peavad LSF § 5a kohaselt olema märgitud:

1) informatsiooni kogumise eesmärk;
2) signaalikandjad, millele juurdepääs on informatsiooni kogumiseks vajalik;
3) otsingumõisted, või nende kategooriad, mida võib informatsiooni hankimisel kasutada;
4) loa kehtivuse aeg (maksimaalselt 6 kuud, misjärel saab luba 6 kuu kaupa pikendada);
5) muud tingimused, mis on vajalikud üksikisiku puutumatuse kaitseks.

Kaitseteabekohtu koosseis ja menetlus on reguleeritud LFR-s. Kaitseteabekohtu esimees määratakse üldise kohtunike määramise korra järgi ja ülejäänud liikmed määrab valitsus (LFR § 2). Valitsus määrab ka juristi, kes esindab menetluses üksikisikute huvi eraelu kaitsele (LFR §-d 5–8).

[65] European Union Agency for Fundamental Rights. Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU, 2015, lk 64. Kättesaadav: http://fra.europa.eu/sites/default/files/fra_uploads/fra-2016-surveillance-intelligence-services_en.pdf

4.4. Järelevalve korraldus julgeoleku- ja luureasutuste tegevuse õigus- ja eesmärgipärasuse üle

4.4.1. Järelevalve Kaitsepolitsei tegevuse üle

Ex ante korras teostab Kaitsepolitsei tegevuse üle järelevalvet kohus, andes loa teatud meetmete kasutamiseks. Kohtu järelevalvet on kirjeldatud eelnevas alapeatükis.

Ex post järelevalvet Kaitsepolitsei üle teostab **Julgeoleku ja Isikuandmete Kaitse Komisjon** (*Säkerhets- och integritetsskyddsnämnden*, SIN), mille tegevust reguleerib LBV. Komisjon teostab järelevalvet kuritegevuse vastu võitlevate organite (sh Kaitsepolitsei) poolt kasutatavate salajaste jälitustoimingute, muudetud identiteetide ja sellega seotud tegevuse üle (LBV § 1). Komisjon teostab järelevalvet inspekteerimise ja muude uurimistegevuste abil ning võib avaldada arvamust olukorra ja tema hinnangul vajalike muutuste kohta ning peab aitama kaasa võimalike puuduste kõrvaldamisele (LBV § 2). Isiku taotlusel on komisjonil kohustus kontrollida, kas isiku suhtes on rakendatud jälitustoiminguid või kas politseiasutused on töödelnud tema isikuandmeid ning kas see on toimunud seadusega kooskõlas. Komisjon teavitab isikut siiski vaid kontrolli läbiviimisest, kuid mitte kontrolli tulemustest (LBV § 3). Raadioluureameti üle teostab sarnast järelevalvet Riiklik Kaitseteabe Inspektsioon.

Erinevalt paljudest teistest Euroopa Liidu liikmesriikides, ei ole Rootsis eraldi julgeolekuasutuste jaoks loodud parlamendikomisjoni, vaid järelevalvet teostavad üldisema suunitlusega parlamendikomisjonid.[66] Kaitsepolitsei tegevuse üle teostavad järelevalvet kaks parlamendikomisjoni: **põhiseaduslikkuse komisjon (***Konstitutionsutskottet***)** ja **õiguskomisjon** (*Justitieutskottet*) (RO ptk. 7, § 8 ja seaduse lisa, p-d 1 ja 4). Mõlemad komisjonid on praktikas korduvalt Kaitsepolitsei tegevust uurinud.[67] RO-s on sätestatud ainult parlamendikomisjoni tegevusvaldkonnad ning puuduvad täpsemad sätted julgeolekuasutuste üle järelevalve teostamise kohta.

Kaitsepolitsei tegevuse üle teostab järelevalvet ka **parlamentaarne ombudsman**, kelle ülesannete hulka kuulub kõikide täitevvõimu organite üle järelevalve teostamine (LRO § 2). Ombudsman teostab järelevalvet selle üle, kas haldusorganite tegevus vastab erapooletuse ja objektiivsuse nõudele ja kas tegevuse käigus ei rikuta isikute põhiõigusi ja –vabadusi (LRO § 3). Ombudsman on oma praktikas Kaitsepolitseid kritiseerinud, kuid ombudsmani üldine lähenemine on see, et ta väldib nö „operatiivsete otsuste“ uurimist.[68]

Andmekaitse Inspektsioon (*Datainspektionen*) teostab järelevalvet Kaitsepolitsei poolt isikuandmete töötlemise üle samamoodi nagu kõigi teiste isikuandmeid töötlevate asutuste puhul (LSF § 10).

4.4.2. Järelevalve välisluurega tegelevate asutuste tegevuse õiguspärasuse tagamiseks

(a) Järelevalve välisluurealase tegevuse üle üldiselt

Välisluure alase tegevuse üle teostab järelevalvet **Riiklik Kaitseteabe Inspektsioon** (*Statens inspektion för försvarsunderrättelseverksamheten*, SIUN) (FSIF § 1). Inspektsioon teostab järelevalvet ka isikuandmete töötlemise üle välisluurealase tegevuse käigus (FSIF § 3). Järelevalve seisneb FSIF § 4 kohaselt järgnevas:

1) LF ja FFV täitmise kontrollimine;
2) kontrollimine, et välisluuret teostatakse kooskõlas valitsuse sätestatud välisluure alase suunaga;

---

[66] European Union Agency for Fundamental Rights. Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU, 2015, lk 34. Kättesaadav: http://fra.europa.eu/sites/default/files/fra_uploads/fra-2016-surveillance-intelligence-services_en.pdf

[67] I. Cameron. Annex A: Country case studies. Parliamentary and specialised oversight of security and intelligence agencies in Sweden, lk 278 Kättesaadav: http://www.europarl.europa.eu/document/activities/cont/201109/20110927ATT27674/20110927ATT27674EN.pdf

[68] Ibid, lk 279.

3) informatsiooni tehnilise ja isikupõhise hankimise erimeetodite kasutamise kontrollimine;
4) muude informatsiooni kogumise meetmete ja meetodite kontrollimine;
5) personali koolitamise ja värbamise põhimõtete kontrollimine.

Riiklik Kaitseteabe Inspektsioon esitab järelevalvetegevuse tulemusena koostatud arvamused ja ettepanekud kontrollitavatele asutustele ja vajadusel ka valitsusele. Inspektsioon esitab iga aasta 1. märtsiks valitsusele ülevaate eelmisel aastal läbi viidud järelevalvetegevuste kohta (FSIF § 5). Inspektsiooni liikmeteks on esimees ja aseesimees, kes peavad olema kohtunikud või endised kohtunikud, ning parlamendierakondade nimetatud liikmed (LSF § 10).

Sarnaselt Kaitsepolitseile, teostavad välisluurega tegelevate asutuste üle järelevalvet kaks **parlamendikomisjoni** (põhiseaduslikkuse- ja õiguskomisjon) ning **parlamentaarne ombudsman**. Kaitsejõudude tegevuse üle on parlamentaarse ombudsmani järelevalve piiratud: ombudsman teostab järelevalvet ainult teise leitnandi auastme või kõrgema auastmega isikute üle (LRO § 2).

Andmekaitse Inspektsioon (*Datainspektionen*) teostab järelevalvet isikuandmete töötlemise üle kaitseluurega tegelevate asutuste poolt samamoodi nagu kõigi teiste isikuandmeid töötlevate asutuste puhul.[69]

(b) Järelevalve Raadioluureameti tegevuse üle

Ex post järelevalvet Raadioluureameti tegevuse üle teostavad **Riiklik Kaitseteabe Inspektsioon** (*Statens inspektion för försvarsunderrättelseverksamheten*, SIUN, LSF §-d 10, 10a), **Isikupuutumatuse Kaitsenõukogu** (*Integritetsskyddsråd*, LSF § 11) ja **Andmekaitse Inspektsioon (***Datainspektionen*, LFRF § 2)[70].

Riiklik Kaitseteabe Inspektsioon kontrollib signaalluureseaduse täitmist ning sel on õigus võtta vastu otsuseid teatud informatsiooni kogumise lõpetamise või kogutud informatsiooni salvestamise või hävitamise kohta, kui ilmneb, et informatsiooni kogumine ei toimunud kooskõlas selleks antud loaga (LSF § 10).

Riiklik Kaitseteabe Inspektsioon on valitsusasutus, mille esimees ja aseesimees peavad olema kohtunikud või endised kohtunikud. Ülejäänud inspektsiooni liikmed esitavad parlamendierakonnad. Liikmed määrab valitsus (LSF § 10).

Isiku taotlusel on inspektsioonil kohustus kontrollida, kas isikut puudutavaid andmeid on signaalluure käigus kogutud ning kas kogumine on toimunud seadusega kooskõlas. Inspektsioon teavitab isikut siiski vaid kontrolli läbiviimisest, kuid mitte kontrolli tulemustest (LSF § 10 a).

Kaitsepolitsei üle teostab sarnast järelevalvet Julgeoleku ja Isikuandmete Kaitse Komisjon.

Isikupuutumatuse Kaitsenõukogu kuulub Raadioluureameti koosseisu ning selle ülesandeks on teostada jooksvat kontrolli isikupuutumatust tagavate meetmete rakendamise üle signaalluure teostamise käigus. Isikupuutumatuse Kaitsenõukogu liikmed määrab valitsus. Isikupuutumatuse Kaitsenõukogu annab oma tegevusest aru Raadioluureametile ja vajadusel Riiklikule Kaitseteabe Inspektsioonile (LSF § 11).

Raadioluureametil on kohustus määrata **andmekaitseametnik**, kelle ülesandeks on jälgida, et isikuandmete töötlemine Raadioluureametis toimub seaduspäraselt ja vastavalt heale tavale ning juhtida tähelepanu võimalikele puudustele. Kui puudusi ei kõrvaldata piisavalt kiiresti, on andmekaitseametnikul kohustus informeerida Andmekaitse Inspektsiooni (LFRF 4. ptk, §-d 1, 2).

Andmekaitse Inspektsioon teostab samuti järelevalvet isikuandmete töötlemise üle Raadioluureameti tegevuse käigus (LFRF 5. ptk § 1). Andmekaitse Inspektsioonil on järelevalve teostamiseks õigus saada:

1) juurdepääs töödeldavatele isikuandmetele;

[69] European Union Agency for Fundamental Rights. Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU, 2015, lk 47. Kättesaadav: http://fra.europa.eu/sites/default/files/fra_uploads/fra-2016-surveillance-intelligence-services_en.pdf
[70] Ibid, lk 30.

2) informatsiooni isikuandmete töötlemise kohta ja juurdepääs isikuandmete töötlemist ja selle turvalisust käsitlevale dokumentatsioonile ja
3) juurdepääs sellistele ruumidele, millised on seotud isikuandmete töötlemisega (LFRF 5. ptk, § 2).

Kui inspektsioon tuvastab, et Raadioluureamet töötleb isikuandmeid ebaseaduslikult, peab ta sellele tähelepanu juhtima. Ebaseaduslikul viisil töödeldud isikuandmete kustutamiseks on inspektsioonil õigus esitada kaebus halduskohtule (LFRF 5. ptk, § 3–4).

4.5. Julgeoleku- ja luureasutuste volitused ja meetmed elektroonilise side jälgimisel ning andmete töötlemisel ja talletamisel

Elektroonilise side jälgimiseks, sh elektroonilise side peatkuulamiseks ja jälgimiseks on volitatud nii Kaitsepolitsei kui ka Raadioluureamet. Kaitsepolitseiameti elektroonilise side salajane pealtkuulamine ja jälgimine ennetuseesmärgil hõlmab ainult selle isiku telefoninumbrit või elektroonilist sidevahendit, kelle suhtes on alust arvata, et ta paneb kuriteo toime ja telefoninumbrit või elektroonilist sidevahendit, mille suhtes on eriline põhjus arvata, et eelpool nimetatud isik nendega ühendust võtab (LSAB § 2, RGB ptk 27 § 20).

Kaitsepolitseil on õigus teatud kuritegude ärahoidmiseks, ennetamiseks või avastamiseks, samuti uurimiseks saada juurdepääs elektroonilise side andmetele (sõnumiedastamise faktiga seotud andmetele) (LBMU §-d 2 ja 3, LEK 6. ptk § 22, RGB 27. ptk § 19).

Raadioluureametil on volitus teostada üldist elektroonilise side jälgimist ehk signaalluuret, st otsingusõnadel põhinevat üldist jälgimist, mis ei ole suunatud konkreetsete isikute jälgimisele (nn massijälgimist). Mõlema asutuse volitusi ja meetmeid ja nende kasutamise protseduure elektroonilise side jälgimisel on kirjeldatud eelmistes alapeatükkides.

4.6. Järeldused läbivate üldpõhimõtete kohta julgeoleku- ja luureasutuste tegevuse reguleerimisel ning elluviimisel

Põhiõiguste kaitsele pööratakse Rootsi julgeoleku- ja luureasutuste tegevust reguleerivates õigusaktides palju tähelepanu. Seda näitab erinevate järelevalveasutuste hulk. Kaitsepolitsei rakendatavate meetmete puhul on isikute põhiõigused suuremal määral kaitstud, kui välisluurega tegelevate asutuste rakendatavate meetmete puhul. Seda seetõttu, et välisluurega tegelevate asutuste rakendatavaid meetmeid ja nende rakendamise aluseid ei ole õigusaktides täpselt reguleeritud. Erandiks on Raadioluureameti teostatav signaalluure, mis on küll detailselt reguleeritud, kuid mis oma üldise iseloomu tõttu riivab juba olemuslikult suurel määral isikute põhiõigusi.

Rootsi julgeoleku- ja luureasutuste järelevalvet puudutava regulatsiooni puhul on kritiseeritud enim seda, et valitsusel on järelevalve teostamisel liiga suur roll. Eelkõige saab siin näitena tuua Riikliku Kaitseteabe Inspektsiooni ja Julgeoleku ja Isikuandmete Kaitse Komisjoni, mis on põhilised julgeolekuasutuste üle järelevalvet teostavad organid ning mille liikmed määrab valitsus. Samas määrab valitsus ka välisluure teostamise suuna. ÜRO inimõiguste komitee on kritiseerinud Rootsis elektroonilise side jälgimise üle teostatavat järelevalvet, märkides, et valitsusel on järelevalve teostamisel laiaulatuslikud volitused ning Rootsi peaks garanteerima, et elektroonilise side jälgimise üle teostaks järelevalvet asutus, millel on piisav erapooletuse ja efektiivsuse garantii.[71] Euroopa Liidu Põhiõiguste amet on toonud välja, et järelevalve julgeolekuasutuste üle ei tohi piirduda valitsuse teostatava järelevalvega[72] ning et Rootsit võib välja tuua riigina, kus kontrollijad ja kontrollitavad

[71] UN, Human Rights Committee, Concluding observations on the sixth periodic report of Sweden, CCPR/C/SWE/CO/6, 7 May 2009.
[72] European Union Agency for Fundamental Rights. Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU, 2015, lk 34. Kättesaadav: http://fra.europa.eu/sites/default/files/fra_uploads/fra-2016-surveillance-intelligence-services_en.pdf

asutused ei ole piisavalt eristatud[73]. Akadeemilises kirjanduses on samuti valitsuse liialdast rolli järelevalve teostamisel kritiseeritud.[74] Privacy International hinnangul ei ole järelevalve signaalluure teostamise üle efektiivne.[75]

Euroopa Liidu Põhiõiguste Amet on kritiseerinud Rootsis parlamendikomisjonide teostavat järelevalvet, täpsemalt seda, et julgeoleku eesmärgil informatsiooni kogumise üle teostavad järelevalvet üldise suunitlusega komisjonid. Üldistel komisjonidel ei ole ameti hinnangul tihti piisavalt aega, et julgeolekualaste spetsiifiliste küsimustega tegeleda ning samuti ei ole selliste komisjonide liikmed tihti piisavalt informeeritud.[76]

Privacy International on tugevalt kritiseerinud Rootsi signaalluure teostamise korda. Organisatsiooni hinnangul ei ole piisavalt tagatud, et Raadioluureameti teostatav signaalluure on fokuseeritud julgeolekuohtudele ning on oht, et Raadioluureamet teostab elektroonilise side üldist jälgimist. Samuti kritiseerib organisatsioon seda, et signaalluure teostamise kord diskrimineerib isikuid kodakondsuse põhjal – signaalluure ei ole Rootsi õiguse kohaselt lubatud kui signaali saaja ja vastuvõtja asuvad mõlemad Rootsis – kuigi ÜRO organid on leidnud, et selline erinev kohtlemine on rahvusvahelise õigusega vastuolus. Samas ei ole eelpool toodud diskrimineerival reeglil praktikas suurt tähtsust, sest Privacy International andmetel käsitletakse välissuhtlusena, mille jälgimine on lubatud, Rootsis asuvate isikute suhtlust läbi teenuste nagu Google ja Facebook. Õigusnormid signaalluure teel kogutud informatsiooni jagamise kohta välisriikidega ei ole Privacy International hinnangul läbipaistvad.[77]

4.7. Rootsi ja Eesti regulatsioonide võrdlus

Julgeolekuasutustega seonduv regulatsioon on Eestis ja Rootsis killustatud ning sisaldub paljudes õigusaktides.

Julgeolekuasutuste süsteemi erinevuseks on see, et erinevalt Eestist ei ole Rootsi õiguses sätestatud „julgeolekuasutuse“ mõistet. Sellest tulenevalt ei ole Rootsis ka üldist julgeolekuvaldkonda reguleerivat seadust, nagu Eestis on julgeolekuasutuste seadus.

Rootsi õiguses on eristatud Kaitsepolitsei tegevus julgeolekualaste kuritegude vastases võitluses ja välisluurega tegelevate asutuste tegevus. Raadioluureamet on küll välisluurealase tegevuse seaduse (2000:130) kohaselt välisluurega tegelev asutus, kuid võib samas signaalluuret läbi viia ka Kaitsepolitsei taotlusel. Nii Rootsis kui Eestis ei ole sõjaliste ja mittesõjaliste julgeolekuasutuste ülesanded selgelt eristatavad ning on mitmeti kattuvad. Üldjoontes on Kaitsepolitsei ülesanded Eestis ja Rootsis samad. Mõlemas riigis täidavad need asutused ka politseifunktsioone. Signaalluure teostamiseks on Rootsis erinevalt Eestist ette nähtud eraldi asutus – Raadioluureamet. Rootsis ei ole Teabeameti sarnast asutust, mille ülesandeks on julgeolekualase teabe kogumine üldiselt.

Julgeolekuasutuste ülesanded, volitused ja meetmed üldiselt Eestis ja Rootsis sarnased, olulise erinevusena saab välja tuua vaid signaalluure teostamise regulatsiooni.

Signaalluure teostamine on Rootsis reguleeritud palju detailsemalt kui Eestis. Raadioluureametil on laiemad elektroonilise side jälgimise volitused, kui ühelgi Eesti julgeolekuasutusel. Raadioluureamet võib Kaitseteabekohtu loal jälgida elektroonilise side signaale otsingusõnade põhjal, st jälgides korraga paljude isikute elektroonilise side signaale. Eelduslikult on Raadioluureametil lubatud ka sõnumite sisu

[73] *Ibid*, lk 71.
[74] European Parliament. National programmes for mass surveillance of personal data in EU Member States and their compability with EU law, 2013, lk 61-62. Kättesaadav: http://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/493032/IPOL-LIBE_ET(2013)493032_EN.pdf
[75] Privacy International. The Right to Privacy in Sweden. 2016, lk 7-9. Kättesaadav: https://www.privacyinternational.org/sites/default/files/UPR_Sweden.pdf
[76] European Union Agency for Fundamental Rights. Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU, 2015, lk 38. Kättesaadav: http://fra.europa.eu/sites/default/files/fra_uploads/fra-2016-surveillance-intelligence-services_en.pdf
[77] Privacy International. The Right to Privacy in Sweden. 2016, lk 3-6. Kättesaadav: https://www.privacyinternational.org/sites/default/files/UPR_Sweden.pdf

jälgimine, kuna seadus ei täpsusta, millise sisuga signaale Raadioluureamet jälgida võib. Ka näiteks Privacy International organisatsioon heidab Rootsile ette, et Raadioluureametil on elektroonilise side nö massijälgimise õigus.[78] Eestis on elektroonilise side sõnumite sisu jälgimine halduskohtu loal lubatud ainult kindlaks määratud isikute suhtes.

Erinevus signaalluure teostamisel seisneb ka selles, et Raadioluureamet teostab signaalluuret vastavalt valitsuse kindlaksmääratud välisluure suunale ning teiste julgeolekuasutuste taotlustele, mitte omal algatusel.

Välisluurega tegelevate asutuste volituste ja meetmete osas on erinevuseks, et Rootsis on detailsemalt reguleeritud ainult signaalluure teostamine. Muid välisluure teostamise meetmed Rootsis õiguses täpsemalt reguleeritud ei ole, vaid välisluurealase tegevuse seaduse (2000:130) §-s 2 on sätestatud ainult, et välisluure käigus kasutatakse tehnilist ja isikupõhist informatsiooni hankimist. Eestis on kaitseväe korralduse seaduses reguleeritud ka Kaitseväe kasutatavad meetmed.

Võrreldes Eesti õigusega ei näe Rootsi õigus julgeolekuasutustele selgelt ette võimalust tegutseda väljapool Rootsi territooriumi.

Kui Eestis piirdub julgeolekuasutuste poolt isikuandmete töötlemise teemaline eriregulatsioon üldise volitusega isikuandmete töötlemiseks, siis Rootsis on nii Raadioluureameti, politsei kui ka Kaitsejõudude tegevuses isikuandmete töötlemise kohta vastu võetud eraldi seadused.

Põhiõiguste riive õiguspärasuse tagamiseks sätestatud protseduuride osas on sarnane, et mõlema riigi seadused piiritlevad kuriteod, mille uurimiseks Kaitsepolitsei jälitustoiminguid kasutada võib.

Nii Rootsis kui ka Eestis on elektroonilise side salajaseks pealtkuulamiseks ja jälgimiseks, salajaseks videovalveks, saadetiste uurimiseks ja konfiskeerimiseks kuritegude ennetamisel ja uurimisel vajalik kohtu luba. Võrreldes Eestiga on Rootsi regulatsiooni erinevuseks, et kuritegude ennetamiseks ei ole lubatud kasutada pealtkuulamist tehniliste seadmete abil. Samuti on Rootsis loodud signaalluure teostamiseks loa andmiseks erikohus, milleks on Kaitseteabekohus. Eestis regulatsioonist erineb ka see, et nii signaalluureks kui ka teisteks jälitustoiminguteks loa taotlemisel osaleb Rootsis menetluses jurist, kes esindab üksikisikute huvisid. Seega on võrreldes Eestiga meetmete kasutamiseks tugevam eelkontroll.

Kui Eestis on üldreegliks, et jälitustoimingutest tuleb isikut teavitada, siis Rootsi õiguses on ette nähtud, et julgeolekualaste kuritegude uurimiseks kasutatud jälitustoimingutest ei tule isikut teavitada. Raadioluureametil on üldpõhimõttena kohustus isikut teavitada, kui signaalluure käigus on kasutatud otsingutermineid, mis seonduvad konkreetse isikuga, kuid teavitamiskohustust ei ole muuhulgas juhul, kui teabe edastamist takistab selle salastatus.

Julgeolekuasutuste järelevalve süsteem erineb Eestis ja Rootsis oluliselt.

Kui Eestis on spetsialiseerunud järelevalveasutuseks Riigikogu julgeolekuasutuste järelevalve komisjon, siis Rootsis toimub järelevalve eelkõige valitsuse kontrolli all olevate asutuste kaudu. Parlamendikomisjonid teostavad ka Rootsis julgeolekuasutuste üle järelevalvet, kuid selleks ei ole loodud spetsiaalset parlamendikomisjoni nagu Eestis, vaid järelevalvet teostavad põhiseaduslikkuse komisjon ja õiguskomisjon. Lisaks on Rootsis mitu julgeolekuasutuste üle järelevalve teostamisele spetsialiseerunud asutust – Kaitseteabekohus, Riiklik Kaitseteabe Inspektsioon, Isikupuutumatuse Kaitsenõukogu ning Julgeoleku ja Isikuandmete Kaitse Komisjon. Eestis sellised spetsialiseerunud institutsioonid (peale Riigikogu komisjoni) puuduvad.

Riigikogu komisjoni poolt (Eestis) ning Riikliku Kaitseteabe Inspektsiooni ja Julgeoleku ja Isikuandmete Kaitse Komisjoni (Rootsis) teostatav järelevalve on sarnane. Kõik nimetatud asutused koostavad mittesiduvaid arvamusi ja ettepanekuid neile esitatud informatsiooni põhjal ehk teostavad võrdlemisi „pehmet“ järelevalvet.

Teistsuguse mehhanismina, mis Eestis puudub, on Rootsis isikutele antud võimalus esitada Julgeoleku ja Isikuandmete Kaitse Komisjonile või Riiklikule Kaitseteabe Inspektsioonile taotlus, et asutused

[78] Privacy International. The Right to Privacy in Sweden. 2016, lk 3-6. Kättesaadav: https://www.privacyinternational.org/sites/default/files/UPR_Sweden.pdf

kontrolliks, kas isikut puudutavaid andmeid on jälitustegevuse käigus kogutud ning kas kogumine on toimunud seadusega kooskõlas. Asutused teavitavad isikut kontrolli läbiviimisest, kuid mitte selle tulemustest.

Nii Eestis kui ka Rootsis teostab julgeolekuasutuste tegevuses isikute põhiõiguste ja –vabaduste järgimise üle järelevalvet ombudsman (Eestis õiguskantsler). Erinevalt Eestist teostab Rootsis julgeolekuasutuste üle järelevalvet ka Andmekaitse Inspektsioon.

Kokkuvõttes järgivad nii Eesti kui ka Rootsi regulatsioon sarnaseid üldpõhimõtteid, sh seda, et julgeolekuasutuste ülesannete täitmisel võib kasutada erinevaid meetmeid, mis piiravad isikute põhiõiguseid. Samas näevad mõlema riigi regulatsioonid ette põhimõtted (proportsionaalsuse põhimõte) ning kontrollimehhanismid (tagatised) põhiõiguste kaitseks.

5. SOOME

5.1. Ülevaade julgeoleku- ja luureasutuste tegevust reguleerivatest õigusaktidest

Soomes on kaks julgeoleku- ja luureasutust: **Soome Kaitsepolitsei** (*Suojelupoliisi*, edaspidi: ***SUPO***) ja **Kindralstaabi Luureosakond** (*Pääesikunnan Tiedusteluosasto*, edaspidi: ***PVTK***), mille tegevust reguleerivad erinevad õigusaktid.

SUPO toimimist politseiasutusena reguleerib politseihalduse seadus (*laki poliisin hallinnosta* 110/1992, edaspidi: *LPH*) ja politseihalduse määrus (*asetus poliisin hallinnosta* 15.3.1996/158, edaspidi: *APH*). Lisaks sellele reguleerib SUPO tööd politseiseadus (*poliisilaki* 22.7.2011/872, edaspidi: *PoL*), mis sätestab SUPO peamised volitused kuritegude ennetamiseks ja avastamiseks. SUPO-le kui riigivastase tegevuse uurimisasutusele kohalduvad volitused, mis on sätestatud sunnimeetmete seaduses (*pakkokeinolaki* 22.7.2011/806, edaspidi: *PaL*) ja kriminaaluurimise seaduses (*esitutkintalaki* 22.7.2011/805, edaspidi: *EL*). SUPO volitused terrorismi tõkestamiseks on sätestatud politseiseaduses ja sunnimeetmete seaduses.

SUPO tegevust julgeolekukontrolli valdkonnas reguleerib julgeolekukontrolliseadus (*turvallisuusselvityslaki* 19.9.2014/726, edaspidi: *TL*).

PVTK ülesanded ning meetmed sätestab kaitsejõudude seadus (*laki puolustusvoimista* 11.5.2007/551, edaspidi: *LPV*) ning sõjaväedistsipliini ja kriminaaluurimise seadus (*laki sotilaskurinpidosta ja rikostorjunnasta puolustusvoimissa* 255/2014, 5, edaspidi: *LSRP*).

5.2. Julgeoleku- ja luureasutuste ülesanded, volitused ja meetmed põhiõiguste piiramisel

Soome Kaitsepolitsei (SUPO) ülesanded on järgmised:

1) selliste tegevuste ja kuritegude ennetamine, mis võivad ohustada riiklikku ja ühiskondlikku korda või riigisisest või -välist turvalisust (LPH § 10 lg 1);
2) eelmises punktis nimetatud kuritegude uurimine (LPH § 10 lg 1);
3) üldise valmiduse säilitamine ja arendamine riigi turvalisust ohustava tegevuse tõkestamiseks (LPH § 10 lg 1 teine lause).

Siseministeerium määrab pärast Politseivalitsuse[79] ärakuulamist täpsemalt teemad, millega SUPO tegeleb ning otsustab pärast Politseivalitsuse ärakuulamist vajadusel täpsemalt SUPO ja muude politseiasutuste vahelise ühise tegutsemise ja koostöö ning nendevahelise uurimistöö korralduse (LPH § 10 lg 2).

Peamised teemad, millega SUPO tegeleb, on järgmised:

1) terrorismi tõkestamine, ennetamine ja avastamine;
2) riigi vastu suunatud varjatud luuretegevust tõkestamine, ennetamine ja avastamine;
3) julgeoleku parandamine.[80]

Eelnimetatud SUPO kohustused hõlmavad sealjuures:

1) koostöös teiste asutustega massihävitusrelvade levitamise ärahoidmist;
2) riigi julgeoleku keskkonna analüüsimist;
3) riikliku ja rahvusvahelise teadlikkuse säilitamist selles valdkonnas;

[79] Politseivalitsus on Siseministeeriumile alluv keskushaldusorgan, mis on kõikide politseiasutuste juhtorgan peale kaitsepolitsei.
[80] Kaitsepolitsei põhimäärus (Suojelupoliisin Ohjesääntö, Dnro 130/2016) § 5. Ministry of Defence. Guidelines for developing Finnish intelligence legislation, lk 15. Kättesaadav: http://www.defmin.fi/files/3144/GUIDELINES_FOR_DEVELOPING_FINNISH_INTELLIGENCE_LEGISLATION.pdf

4) riigisisest julgeolekut mõjutava õigusvastase aktiivsuse tõkestamist, ennetamist ja avastamist;
5) ohtude hindamist seoses riigivisiitide ja märkimisväärset tähtsust omavate konverentsidega;
6) luuretegevust SUPO pädevusalas ja
7) nende kuritegude uurimist, mis kuuluvad SUPO pädevusalasse (riiki kahjustavad kuriteod).[81]

SUPO on kohustatud politseihalduse seaduses sätestatud ülesannete täitmiseks andma ametiasutustele ja juriidilistele isikutele selliseid juhiseid, nõuandeid ja teavet, mis on vajalikud riigi turvalisuse hoidmiseks või selle vastu suunatud ründe tõkestamiseks (APH § 8). SUPO peab teavitama tema ülesanneteks olevatest ühiskondlikult olulistest asjadest siseministrit ning lisaks politseipeadirektorit, kui neil asjadel on oluline mõju politsei muule tegevusele (LPH § 4a).

SUPO ennetuslikust julgeolekutööst moodustab ühe osa julgeolekukontrollimenetlus, mis seisneb asutuse või organisatsiooni personali usaldatavuse tugevdamises ja sisejulgeolekule või riigi majandusele ohtu kujutavate kuritegude ennetamises (TL § 9 lg 1) (vastuluure tegevus).

Kindralstaabi Luureosakonna (PVTK) ülesanded on järgmised:

1) Soome maismaa, mereala ja õhuruumi üle järelevalve teostamine ja riigi territoriaalse terviklikkuse kindlustamine;
2) Soome elanikkonna toimetuleku ja põhiõiguste ning valitsuse toimimise ja seadusjärgse ühiskondliku korra kaitse;
3) teistele asutustele toe pakkumine, mis hõlmab:

   a) täidesaatvat abi avaliku korra ja turvalisuse säilitamisel, et ennetada ja tõkestada terroriakte, ning kaitsta ühiskonda tervikuna;

   b) abi päästeoperatsioonidel, pakkudes varustust, personali ja ekspertide teenust;

   c) abiks olemist teistes riikides toimunud terroriaktide, looduskatastroofide, suurte õnnetuste või muu sarnase olukorra puhul; ja
4) osalemine rahvusvahelistes kriisijuhtimisolukordades (LPV § 2).

PVTK luuretegevus on suunatud peamiselt välisriikidele, eriti välisriikide sõjalistele organisatsioonidele.[82] Kaitsejõudude vastuluure tegevus keskendub Soome riiklikku sõjalist kaitset ohustavate kuritegude ennetamisele ja avastamisele.[83]

Lisaks eelnevale on PVTK ülesandeks Soome vastu suunatud luuretegevuse ja sõjalise riigikaitse eesmärki ohustava tegevusega seotud kuritegude ennetamine ja avastamine (LSRP § 86 lg 1). Sealjuures piirneb PVTK pädevus luuretegevusega seotud kuritegude avastamise ja ennetamisega, sest SUPO ülesandeks on selliste kuritegude uurimine (LSRP § 86 lg 2).

Julgeoleku ja luureasutuste volitused ning meetmed on sätestatud politseiseaduses, sunnimeetmete seaduses ning kaitseväeteenistusalase distsiplinaarmenetluse ja kaitsejõududes kuritegudega võitlemise seaduses.

5.2.1. SUPO volitused ja meetmed

SUPO-l on õigus koguda ametiülesannete korras teavet ja vajalikke dokumente avalikku ülesannet täitvalt asutuselt (PoL 4. ptk § 2 lg 1). Kuriteo ennetamiseks või uurimiseks on SUPO-l õigus hankida vajalikku teavet eraõiguslikelt juriidilistelt isikutelt või füüsilistelt isikutelt, vaatamata äri-, pangandus-

[81] Kaitsepolitsei põhimäärus (Suojelupoliisin Ohjesääntö, Dnro 130/2016) § 5. Ministry of Defence. Guidelines, lk lk 18 lg 4, lk 15.
[82] Ministry of Defence. Guidelines, lk 17.
[83] Ministry of Defence. Guidelines, lk 22.

või kindlustusandmete saladusele (PoL 4. ptk § 3 lg 1). Samuti on SUPO-l õigus üksikutel juhtudel sideoperaatoritelt hankida kontaktteavet mitteavalike abonendiandmete kohta (PoL 4. ptk § 3 lg 2).

Ehkki Soome julgeolekuhuvid võivad aeg-ajalt seda vajada, ei ole SUPO-l õigusi laiendada oma teabekogumise õigust välisriikidesse või andmesidevõrkudele.[84]

(a) SUPO meetmed süütegude ennetamiseks ja avastamiseks

SUPO võib kasutada erinevaid salajasi teabe kogumise meetmeid (soome keeles *salaiset tiedonhankintakeinot*) süütegude ennetamiseks ja avastamiseks (PoL 5. ptk § 1 lg 1). Need teabehankimise meetmed on järgmised:

1) elektroonilise side pealtkuulamine[85] (PoL 5. ptk § 5);
2) teabe kogumine muul moel, kui elektroonilise side pealtkuulamisega[86] (PoL 5. ptk § 6 lg 1);
3) elektroonilise side liiklusandmete (meta-andmete) jälgimine[87] (PoL 5. ptk § 8 lg 1);
4) elektroonilise side liiklusandmete jälgimine võrguaadressi või lõppseadme omaniku nõusolekul (PoL 5. ptk § 9);
5) tugijaama andmete kogumine[88] (PoL 5. ptk § 11 lg 1);
6) süstemaatiline jälgimine[89] (PoL 5. ptk § 13 lg 1);
7) varjatud teabehanke teostamine[90] (PoL 5. ptk § 15 lg 1);
8) eluruumi pealtkuulamine tehnilise vahendi abil[91] (PoL 5. ptk § 17 lg-d 1 ja 2);
9) varjatud jälgimise teostamine tehnilise vahendi abil[92] (PoL 5. ptk § 19 lg 1);
10) objekti asukoha ja liikumise jälgimine tehniliste seadmete abil[93] (PoL 5. ptk § 21 lg 1);
11) tehnilise seire teostamine elektrooniliste seadmete üle[94] (PoL 5. ptk § 23 lg 1);

---

[84] Ministry of Defence. Guidelines, lk 24.

[85] Elektroonilise side pealtkuulamine tähendab üldkasutatava sidevõrgu või sellega seotud sidevõrgu kaudu elektroonilisel aadressil või elektroonilise side võrgu lõppseadmes vastu võetava või sellest edastatud sõnumi pealkuulamist, salvestamist ja muud käitlemist sõnumi sisu ja sellega seotud identimisandmete uurimiseks.

[86] Kui on tõenäoline, et elektroonilise side pealtkuulamise objektiks olevat sõnumit ei ole enam võimalik pealt kuulata, võib SUPO kuriteo ennetamiseks koguda sideteenuse pakkujal või ühingust abonendil valduses olevaid andmeid.

[87] Elektroonilise side kontrollimine on sellise sõnumi identimisandmete hankimine, mis on edastatud sidevõrku ühendatud elektroonilise side aadressilt või elektroonilise side lõppseadmest või mis on vastu võetud sellisel aadressil või sellises seadmes ning elektroonilise side aadressi või elektroonilise side lõppseadme asukohaandmete hankimine või elektroonilise side aadressi või elektroonilise side lõppseadme kasutamise ajutine tõkestamine. Identimisandmed on abonendi või kasutajaga seostatavat sõnumit puudutavad andmed, mida sidevõrgus käideldakse sõnumite ülekandmiseks, jaotamiseks või kättesaadaval hoidmiseks.

[88] Tugijaama andmete kogumine tähendab konkreetse tugijaama kaudu kasutatud lõppseadmete ja võrguaadresside andmete hankimist.

[89] Süstemaatiline jälgimine tähendab varjatud jälitustegevuse teostamist kindla isiku suhtes teabe kogumise eesmärgil. Süstemaatiline jälgimine võib hõlmata kaamera või muude tehniliste seadmete abil visuaalse jälgimise salvestamist. Laiendatud süstemaatiline järelevalve tähendab muud kui lühiajalist süstemaatilist jälgimist isiku üle, keda mõistlikul alusel kahtlustatakse kuriteo toimepanemises.

[90] Varjatud teabekogumine on teatud isikule suunatud lühiajaline vastastikuses suhtluses toimuv teabehange, milles politseiametniku ülesande varjamiseks kasutakse ebaõigeid, eksitavad või varjatud andmeid.

[91] Tehnilise vahendi abil toimuv pealtkuulamine on kuriteos kahtlustatava sellise vestluse või sõnumi, mis ei ole suunatud kõrvalistele isikutele ja milles pealtkuulaja ei osale, pealtkuulamine, salvestamine ja muu käitlemine tehnilise vahendi, meetodi või programmiga vestluse või sõnumi sisu või selle poolte või kahtlustatava tegevuse väljaselgitamiseks.

[92] Tehnilise vahendi abil jälgimine tähendab kindla isiku või hoonete või muu asukoha seiret või salvestamist, kasutades kohta paigaldatud kaamerat või muud tehnilist seadet, protsessi või tarkvara osa.

[93] Objekti asukoha ja liikumise jälgimine tähendab eseme, aine või vara liikumise jälgimist, kasutades eraldi selle sisse paigaldatud või juba selles asuvat raadiosaatjat või muud sarnast tehnilist seadet, protsessi või tarkvara.

[94] Tehniline seire seadme üle tähendab muud, kui üksnes sensoorset seiret, arvutis, muus sarnases seadmes või tarkvaras või nende protsessides sisalduvate identimisandmete salvestamist või muud töötlemist kuriteo ennetamiseks vajaliku asjaolu uurimise eesmärgil.

12) elektroonilise side aadressi või elektroonilise side lõppseadme identimisandmete hankimine tehnilise seadme abil (PoL 5. ptk § 25);
13) varjatud tegevuse teostamine[95] (PoL 5. ptk § 28 lg 1);
14) teostada näiliseid tehinguid[96] (PoL 5. ptk § 35 lg 1);
15) teabeallika kasutamine[97] (PoL 5. ptk § 40 lg 1);
16) kontrollitud läbipääs[98] (PoL 5. ptk § 43 lg 1).

SUPO võib kasutada ka üldiseid politseivolitusi, näiteks tuvastada identiteeti (PoL 2. ptk, § 1), siseneda ruumi ja seda läbi otsida (PoL 2. ptk, § 6), vahistada (PoL 2. ptk, § 2-3), teostada turvakontrolli (PoL 2. ptk, § 12), kasutada jõudu (PoL 2. ptk, § 17), kasutada tulirelva (PoL 2.ptk, § 19), peatada sõidukeid (PoL 2. ptk § 11) jne.

Julgeolekukontrollimenetluses ei ole jälitustegevus ega salajaste teabe kogumise meetmete kasutamine lubatud (TL).

(b) SUPO meetmed süütegude menetlemisel

Süütegude menetlemise pädevus on kriminaaluurimisasutusena politseil, sealhulgas piiratud pädevuses SUPO-l (EL 2. ptk § 1 lg-d 1 ja 2). SUPO tegeleb kriminaaluurimisega selle pädevusalasse kuuluvate kuritegude lahendamisel.[99]

SUPO võib oma pädevuses kriminaaluurimise läbiviimisel rakendada suures osas samu meetmeid, mida politseiseaduse alusel kuritegude ennetamiseks ja avastamiseks (PoL 5. ptk § 1 lg 5; PaL 10. ptk). PaL-s nimetatakse neid salajasteks sunnimeetmeteks, mis on järgmised:

1) elektroonilise side pealtkuulamine (PaL 10. ptk § 3 lg 2, eriti p-d 1–3, 11);
2) teabe kogumine muul moel, kui elektroonilise side pealtkuulamisega (PaL 10. ptk § 4);
3) elektroonilise side liiklusandmete jälgimine (PaL 10. ptk § 6 lg 2 p 6);
4) võrguaadressi või lõppseadme asukohateabe hankimine, et saada ühendust kahtlustatava või süüdimõistetuga (PaL 10. ptk § 8);
5) tugijaama andmete kogumine (PaL 10. ptk § 10);
6) süstemaatiline jälgimine (PaL 10. ptk § 12);
7) varjatud teabehanke teostamine (PaL 10. ptk § 14 lg 2 p 6);
8) muu kui eluruumi pealtkuulamine tehnilise vahendi abil (PaL 10. ptk § 16 lg 2 ja lg 3 p 3);
9) eluruumi pealtkuulamine tehnilise vahendi abil (PaL 10. ptk § 17 p-d 1–3, 9);
10) varjatud jälgimise teostamine tehnilise vahendi abil (PaL 10. ptk § 19);
11) objekti asukoha ja liikumise jälgimine tehniliste seadmete abil (PaL 10. ptk § 21);
12) tehnilise seire teostamine elektrooniliste seadmete üle (PaL 10. ptk § 23);
13) elektroonilise side aadressi või elektroonilise side lõppseadme identimisandmete hankimine tehnilise seadme abil (PaL 10. ptk § 25);

---

[95] Varjatud tegevus tähendab laiendatud teabe kogumist kindlate isikute või nende tegevuse kohta. Varjatud tegevuse viisiks on infiltreerumine, mille käigus antakse vale, eksitava või tõest teavet varjava sisuga teavet või tehakse selliseid registrikanded või kasutatakse võltsdokumente, et võita usaldust, mis on vajalik teabekogumiseks või selleks, et vältida teabekogumise paljastamist.

[96] Näiline tehing on tehingu ettepanek või eseme, aine, vara või teenuse ostmine politsei poolt. Näilise tehingu objektiks on ese, mis on seotud ennetatava kuriteoga. Meetme eesmärk on ennetada kuritegu sellega, et politsei võtab endale tehingu objekti valduse või saab teada objekti asukoha.

[97] Teabeallika kasutamine tähendab hankida teabehankega nõustunud isikult väljastpoolt politseid või muud eeluurimisasutust mittejuhuslikku, konfidentsiaalset, kuriteo lahendamise seisukohalt tähtsust omavat teavet.

[98] Politsei võib jätta sekkumata eseme, aine või vara transporti või muul viisil üleandmisesse või viivitada sekkumisega, kui see on vajalik, et tuvastada isikuid, kes on seotud kuriteo toimepanemisega või tõsisema või suurema kuriteo ärahoidmiseks.

[99] Ministry of Defence. Guidelines, lk 18 lg 4.

14) varjatud tegevuse teostamine (PaL 10. ptk § 27);
15) näiliste tehingute teostamine (PaL 10. ptk § 34);
16) teabeallika kasutamine (PaL 10. ptk § 39 lg-d 1, 2);
17) kontrollitud läbipääs (PaL 10. ptk § 41).

SUPO võib kasutada ka üldiseid politseivolitusi, näiteks õigust vahistada (PaL 2. ptk § 1, 2), kehtestada reisikeeldu (PaL 5. ptk § 1), otsida läbi ruume (PaL 8. ptk § 2), avada ja läb vaadata dokumente (PaL 8. ptk § 13), otsida andmeid seadmest (PaL 8. ptk § 21), otsida läbi isikuid (PaL 8. ptk § 31), võtta DNA proove (PaL 9. ptk § 4) jne.

5.2.2. PVTK kasutuses olevad meetmed

PVTK õigused on võrreldes SUPO-ga piiratumad.[100] Kaitsejõududel on lubatud kuritegude ennetamisel ja avastamisel rakendada vaid järgnevaid meetmeid (LSRP § 89 lg 1):

1) tugijaama andmete hankimine (p 1);
2) süstemaatiline jälgimine (p 2);
3) varjatud teabehange (p 3);
4) tehnilise vahendi abil toimuv pealkuulamine (p 4);
5) tehnilise vahendi abil toimuv varjatud jälgimine (p 5);
6) tehnilise vahendi abil toimuv jälitamine (p 6);
7) elektroonilise side aadressi või elektroonilise side lõppseadme identimisandmete hankimine (p 7).

Kaitsejõudude pädeva ametniku[101] kirjalikul taotlusel võib kaitsepolitsei ametiabi korras teha politsei pädevusse kuuluva üksiktoimingu, milleks kaitsejõudude ametnikul volitus puudub (LSRP § 38 lg 1, LSRP § 90 lg 1).

PVTK-l on õigus kuritegude ennetamisel ja avastamisel saada teavet registritest (LSRP § 91) ning ametiasutuselt ja avalikku ülesannet täitma volitatud juriidiliselt ja füüsiliselt isikult (LSRP § 92). Samuti on kaitsejõududes kuritegude ennetamise ja paljastamisega tegelevatel ametnikel õigus saada elektroonilise side ettevõtjatelt ja kollektiivtellijalt kontaktandmed sellise elektroonilise side konto kohta, mida ei ole avalikus loetelus, või elektroonilise side konto, e-posti aadressi, muu elektroonilise side aadressi või elektroonilise side lõppseadme identimisandmed, kui üksikjuhtudel vajatakse andmeid Soome vastu suunatud luuretegevuse ja sõjalise riigikaitse eesmärki ohustava tegevusega seotud kuritegude ennetamise ja paljastamiseks. Kaitsejõududes kuritegude ennetamise ja paljastamisega tegelejatel on õigus saada postiteenust pakkuvalt juriidiliselt isikult adressaatide andmeid (LSRP § 93).

PVTK sõjalist luuretegevust välisriikide vastu samas Soome seadusandlus ei reguleeri. Seda tegevust juhitakse asutusesiseste korralduste ja Kaitsejõudude suunistega.[102]

5.3. Protseduurid põhiõiguste riive õiguspärasuse tagamiseks

5.3.1. SUPO

[100] Ministry of Defence. Guidelines, lk 22.
[101] Kuritegude ennetamisel ja avastamisel on pädevad peastaabi vastuluure eest vastutava osakonnajuhataja asetäitja ametikohale määratud ohvitser ning sõjaväejurist, kuritegude ennetamise ja avastamisega tegelema määratud ohvitser, eriohvitser, õppeasutuse ohvitser, allohvitser (LSRP § 90 lg 1). Kriminaalmenetluses on pädevad ametnikud kaitsejõudude assessor ja sõjaväejurist (LSRP § 38 lg 1).
[102] Ministry of Defence. Guidelines, lk 25 lg 4.

Üldpõhimõtted

Salajaste teabe kogumise meetmete kasutamisel kuritegude ennetamiseks, avastamiseks ning uurimiseks tuleb SUPO-l lähtuda põhiõigustest (PoL 1. ptk § 2) ja proportsionaalsuse põhimõttest, mille kohaselt võib meetmeid kasutada ainult juhul, kui see on õigustatud, arvestades uuritava süüteo raskust, kuriteo väljaselgitamise olulisust, meetmete kasutamisest tekkiva põhiõiguste riive raskust ja teisi juhtumi asjaolusid (PoL 1. ptk § 3, PaL 1. ptk § 2). Samuti peab politseiasutus lähtuma minimaalse sekkumise põhimõttest, mille järgi ei tohi kellegi õigusi riivata rohkem, kui on vajalik püstitatud eesmärgi saavutamiseks (PoL 1. ptk § 4, PaL 1. ptk § 3 lg 1). Salajaste teabe kogumise meetmete kasutamisega ei tohi kaasneda kellelegi põhjendamatu kahju (PaL 1. ptk § 3 lg 2). Säilitada tuleb diskreetsus ning vältida salajaste teabe kogumise meetmete kasutamisega kellelegi põhjendamatu tähelepanu pööramist (PaL 1. ptk § 4).

(a) Salajaste teabe kogumise meetmete kasutamine julgeoleku eesmärgil

SUPO ennetava ja tõkestava tegevuse puhul võib salajasi teabe kogumise meetmeid kasutada eeldusel, et teabekogumise tulemusel saadakse teave süüteo toimepanemise ohu ennetamiseks, avastamiseks või ärahoidmiseks (PoL 5. ptk § 2 lg 1). Enamiku meetmete[103] rakendamisele on täiendav eeldus, et kasutatavatel salajaste teabe kogumise meetmetel on märkimisväärne mõju süüteo ennetamiseks või avastamiseks. Varjatud tegevuse või kontrollitud läbipääsu lubatavuseks on nõutav ka meetme hädavajalikkus kuriteo ennetamiseks või avastamiseks (PoL 5. ptk § 2 lg 2).

SUPO võib kasutada varjatud teabe kogumise meetmeid järgmiste kuritegude avastamiseks:

1) Soome suveräänsuse ohustamine (PoL 5. ptk § 3 p 1);
2) sõja õhutamine (PoL 5. ptk § 3 p 2);
3) riiki kahjustav tegevus, riiki raskelt kahjustav tegevus (PoL 5. ptk § 3 p 3);
4) spionaaž, raske spionaaž (PoL 5. ptk § 3 p 4);
5) riikliku saladuse paljastamine (PoL 5. ptk § 3 p 5);
6) ebaseaduslikud luureoperatsioonid (PoL 5. ptk § 3 p 6);
7) terroriakti toimepanemine (PoL 5. ptk § 3 p 7);
8) terroriakti ettevalmistamine (PoL 5. ptk § 3 p 8);
9) terrorigrupi juhtimine (PoL 5. ptk § 3 p 9);
10) terroristliku liikumise õhutamine (PoL 5. ptk § 3 p 10);
11) terrorikuriteo toimepanemiseks valmistumine (PoL 5. ptk § 3 p 11);
12) terroriakti toimepanemisele värbamine (PoL 5. ptk § 3 p 12);
13) terrorismi rahastamine (PoL 5. ptk § 3 p 13).

SUPO võib kasutada salajasi teabe kogumise meetmeid ka kuritegude tõkestamiseks ja ärahoidmiseks, kuid vastava meetme kasutamine sõltub sellest, milliste kuritegude puhul vastava meetme kasutamine lubatud on (need on sätestatud PoL 5. peatükis vastavate meetmete all). Üldiselt on salajased teabe kogumise meetmed lubatud terrorismi ja ebaseaduslike luureoperatsioonide kuritegude tõkestamiseks. Olukord on keerulisem ja sõltub tõlgendamist, kui meetmeid kasutatakse järgmiste süütegude ennetamiseks: massihävitusrelvade ja kahesuguse kasutusega kaupade levitamine ning riiklikku julgeolekut ohustavad kuriteod, mis on seotud organiseeritud kuritegevusega.[104]

Salajaste teabe kogumise meetmete vajalikkus tähendab ühtlasi seda, et meetmete rakendamine tuleb katkestada enne tähtaega, kui nende kasutamise eesmärk on täidetud või eeldusi nende kasutamiseks enam ei eksisteeri (PoL 5. ptk § 2 lg 3). Kui olukorras, kus salajase teabe kogumise meetmeid

[103] Need meetmed on: elektroonilise side pealtkuulamine; teabe kogumine muul moel, kui elektroonilise side pealtkuulamise teel; varjatud jälitustegevuse teostamine; tehnilise vahendi abil pealtkuulamine väljaspool püsivaks elamiseks kasutatavat ruumi; tehnilise vahendi abil varjatud jälgimine; objekti asukoha ja liikumise jälgimine tehniliste seadmete abil; tehnilise seire teostamine elektrooniliste seadmete üle; varjatud tegevus; näiliste ostude teostamine; teabeallika kaasamine; kontrollitud läbipääs.

[104] Ministry of Defence. Guidelines, lk 20 lg 4.

kasutatakse kuriteo ennetamiseks või avastamiseks, ilmneb, et kuritegu on juba toime pandud, võib jätkata nende meetmetega veel kolme päeva jooksul loa olemasolul ja loa kehtivusaega järgides. Juhul kui salajaste teabe kogumise meetmete kasutamine on vajalik kriminaaluurimises, tuleb taotleda eraldi luba (PoL 5. ptk § 4).

Reeglina otsustab salajaste teabe kogumise meetmete kasutamise **Helsinki Ringkonnakohus**. Näiteks annab kohus loa elektroonilise side pealtkuulamiseks või teabe kogumiseks muul viisil kui side pealkuulamiseks kuni üheks kuuks (PoL 5. ptk § 7 lg 2). Elektroonilise side pealtkuulamise objektiks võib olla vaid kuriteos kahtlustatavalt isikult pärinev või temale suunatud sõnum (PoL 5. ptk § 5).

Ka elektroonilise side liiklusandmete (meta-andmete) jälgimiseks ning nende andmete jälgimiseks võrguaadressi või lõppseadme omaniku nõusolekul, on vaja kohtu luba, mis antakse kuni üheks kuuks (PoL 5. ptk § 10 lg 1, 5, § 9 lg 1 p-d 1, 2, 4). Otsuse elektroonilise side liikluse jälgimise kohta võib ajutiselt teha kuni kohtuotsuse tegemiseni vahistamisõigusega politseiametnik (PoL 5. ptk § 10 lg 2 esimene lause). Avaldus kohtuotsuse taotlemiseks tuleb sellisel juhul esitada esimesel võimalusel, kuid hiljemalt 24 tunni möödumisel tegevuse alustamisest (PoL 5. ptk § 10 lg 2 teine lause).

Kohtu luba on vajalik ka varjatud jälgimine tehnilise vahendi abil (PoL 5. ptk § 19). Meetme kasutamine ei ole reeglina lubatud eluruumides (PoL 5. ptk § 19 lg 2). Eluruumides on võimalik tehnilist pealkuulamist teostada politseikohustuse ohutuks läbiviimiseks ja politseiniku, vahistatu või kaitstava isiku elule ja tervisele avalduva ohu ärahoidmiseks (PoL 5. ptk § 19 lg 5). See antakse kuni kuuks ajaks korraga (PoL 5. ptk § 20 lg-d 1, 3).

Tehnilise vahendi abil pealtkuulamiseks annab loa kohus korraga kuni kuuks ajaks (PoL 5. ptk § 18 lg-d 1, 2). Tehnilise vahendi abil pealtkuulamine ei ole SUPO kuritegusid ennetava ja paljastava ülesande raames reeglina lubatud (PoL 5. ptk § 17 lg 2). Eluruumi võib erandina tehnilise seadme abil pealt kuulata, et tagada politsei ametiülesande ohutu läbiviimine või hoida ära politseiniku, kinnipeetava või kaitse all oleva isiku elule ja tervisele avalduva oht (PoL 5. ptk § 17 lg 5).

Kohtu luba on nõutav ka järgmiste meetmete puhul: tugijaamade kogumine (PoL 5. ptk § 12), objekti asukoha ja liikumise jälgimine tehniliste seadmete abil (luba antakse kuni kuueks kuuks, PoL 5. ptk § 22 lg-d 1, 3), tehnilise seire teostamine elektrooniliste seadmete üle (luba antakse kuni üheks kuuks, PoL 5. ptk § 24 lg-d 1, 2).

SUPO direktor otsustab loa andmise varjatud teabekogumiseks, varjatud tegevuseks (kuni kuueks kuuks)[105], näiliseks tehinguks (kuni kaheks kuuks), teabeallika kasutamiseks (kuni kuueks kuuks) ja kontrollitud läbipääsuks (kuni üheks kuuks) (PoL 5. ptk § 16 lg 1, § 32 lg 1, § 36 lg 1, § 42 lg 1, § 44 lg 1). SUPO direktor võib otsustada ka võrguaadressi või lõppseadme kasutamise ajutise takistamise, et ära hoida tõsist ohtu elule või tervisele (PoL 5. ptk § 10 lg 3). Kui meetme kasutamisega sellisel juhul ei ole võimalik viivitada, võib kuni SUPO direktori loani teha otsuse ka vahistamisõigusega politseiametnik (PoL 5. ptk § 10 lg 3 teine lause).

Vahistamisõigusega politseiametnik[106] otsustab elektroonilise side liiklusandmete jälgimise, kui meede on hädavajalik elule või tervisele avalduva vahetu ohu ärahoidmiseks või kui meetme kasutamiseks on omaniku nõusolek ja isikut kahtlustatakse kuriteos, mis viib võrguaadressi või lõppseadme ebaseadusliku valdamiseni teise isiku poolt (PoL 5. ptk § 10 lg 4). Vahistamisõigusega isikul on õigus otsustada võrguaadressi või lõppseadme identimisandmete hankimise üle (PoL 5. ptk § 25 lg 3). SUPO võib elektroonilise side aadressi või elektroonilise side lõppseadme identimisandmete hankimisel kasutada seadmeid, mida on võimalik kasutada üksnes võrguaadresside ja lõppseadmete identimiseks. Meetme käigus kasutatavaid seadmeid kontrollib eelnevalt pädev asutus[107], et tagada seadme vastavus sätestatud piirangutele ja kindlustada, et seade ei kahjusta üldkasutatavate sidevõrkude varustust või teenuseid (PoL 5. ptk § 25 lg 2). Väljaspool eluruume võib politseiametnik seadmete, protsesside või tarkvara osade installeerimiseks, algatamiseks või lõpetamiseks siseneda varjatult ja

[105] Varjatud tegevus eluruumides on lubatud ainult juhul, kui sinna sisenemine või seal viibimine toimub seal elava isiku aktiivsel tegutsemisel (PoL 5. ptk § 28 lg 4).
[106] Vahistamisõigusega politseiametnikud loetleb PaL 2.ptk § 9.
[107] Soomes sideteenuseid reguleeriv asutus (The Finnish Communications Regulatory Authority)

objekti omaniku tahte vastaselt objektile (PoL 5. ptk § 26 lg 1). Eluruumide puhul see reeglina lubatud pole (PoL 5. ptk § 26 lg 1).

Samuti otsustab vahistamisõigusega politseiametnik laiendatud süstemaatilise jälgimise (korraga 6 kuuks, PoL 5. ptk § 14). Süstemaatilist jälgimist ei tohi teostada eluruumis (PoL 5. ptk § 13 lg 4 esimene lause) ning sellel teostamiseks ei või kasutada tehnilisi seadmeid (PoL 5. ptk § 13 lg 4 teine lause).

Isiku teavitamine kuritegude ennetamisel ja avastamisel

SUPO peab kuritegude ennetamisel ja avastamisel teavitama isikut salajaste teabe kogumise meetmete kasutamisest (EL 4. ptk § 15 lg 5). Isikut tuleb teavitada kirjalikult viivitamata hiljemalt üks aasta pärast asja saatmist prokurörile või kriminaalmenetluse lõpetamist muul põhjusel, kui tegu on järgmiste meetmetega:

1) elektroonilise side pealtkuulamisega;
2) teabe kogumisega muul viisil, kui elektroonilise pealtkuulamisega;
3) elektroonilise side liikluse jälgimisega;
4) süstemaatilise jälitusega;
5) varjatud teabehankega;
6) tehnilise seadme abil jälitamisega;
7) kontrollitud läbipääsuga (PoL 5. ptk § 58 lg 1).

Kohtu otsusel võib eelnimetatud juhtudel teavitamise edasi lükata kuni kahe aasta võrra, kui selle põhjuseks on hetkel või tulevikus toimuva teabekogumise turvalisuse, riigi turvalisuse või elu ja tervise kaitse (PoL 5. ptk § 58 lg 2).

Isikut ei ole vaja teavitada, kui läbi ei viida kriminaaluurimist ning kasutatakse järgmisi meetmeid:

1) laiendatud süstemaatilisest jälgimist;
2) varjatud teabehanget;
3) varjatud tegevust;
4) näilist tehingut;
5) kontrollitud läbipääsu (PoL 5. ptk § 58 lg 5).

Viivitamisel või teavitamata jätmisel peab asutus kaaluma kahtlustatava õigusi (PoL 5. ptk § 58 lg 6). Näilist tehingut ja teabeallika kasutamist puudutava teavitamise otsustab Helsinki Ringkonnakohus (PoL 5. ptk § 58 lg 7).

Teavitamise järel on isikul õigus saada teavet dokumentide või salvestiste kohta, mis toimingu käigus tehtud on, kui avaldamata jätmine ei ole põhjendatud riigi turvalisuse, elu, tervise ja turvalisuse kaitse, taktikaliste või tehniliste protseduuridega, mida hoitakse salajasena. Teabe andmata jätmisest tuleb isikut teavitada (PoL 5. ptk § 60 lg 2).

(b) SUPO salajaste sunnimeetmete kasutamine süütegude menetlemisel

Kriminaalmenetluses on erinevate meetmete kasutamise esmaseks eelduseks see, et nende kasutamine annab teavet, mida on vaja süüteo uurimise lahendamiseks (PaL 10. ptk § 2 lg 1). Enamike meetmete[108] kasutamine on lubatud, kui see on äärmiselt oluline kriminaaluurimise lahendamiseks. Isikute õigusi intensiivselt riivavaid meetmeid[109] võib kasutada, kui need on vajalikud asja lahendamiseks (PaL 10. ptk § 2 lg 2). Salajaste sunnimeetmete (salajaste teabe kogumise meetmete) kasutamine tuleb lõpetada enne tähtaega, kui nende kasutamise eesmärk on täidetud või lõppenud (PaL 10. ptk § 2 lg 3).

[108] Need meetmed on: elektroonilise side pealtkuulamine; teabe kogumine muul moel, kui elektroonilise side pealtkuulamisega; laiendatud süstemaatiline jälgimine; pealtkuulamine tehnilise vahendi abil väljaspool püsivaks elamiseks kasutatavat ruumi; tehnilise vahendi abil varjatud jälgimine; objekti asukoha ja liikumise jälgimine tehniliste seadmete abil; tehniline seire elektrooniliste seadmete üle; varjatud tegevus; näiline tehing; teabeallika kasutamine; kontrollitud läbipääs.

[109] Varjatud tegevus, näiline tehing, tehnilise vahendi abil eluruumis pealtkuulamine.

Salajaste teabe kogumise meetmete kasutamiseks annab loa reeglina Helsinki ringkonnakohus (PoL 5. ptk § 45 lg 1). Olukorras, kus otsustatakse kuulata isikut pealt eluruumis, peab kohus nimetama kahtlustatavale riikliku esindaja, kelle ülesanne on kaitsta kahtlustatava huvisid (PaL 10. ptk § 44 lg 1).

SUPO direktor otsustab loa andmise varjatud teabehankeks, varjatud tegevuseks, näiliseks tehinguks, teabeallika kasutamiseks ja kontrollitud läbipääsuks (PaL 10. ptk § 15 lg 1, § 31 lg 1, § 35 lg 1, § 40 lg 1, § 42 lg 1).

Vahistamisõigusega politseiametnik otsustab elektroonilise side liiklusandmete jälgimise, kui meetme kasutamiseks on omaniku nõusolek ja isikut kahtlustatakse kuriteos, mis viib võrguaadressi või lõppseadme ebaseadusliku valdamiseni teise isiku poolt (PaL 10. ptk § 9 lg 2). Samuti otsustab vahistamisõigusega ametnik laiendatud süstemaatilise jälgimise, mitteeluruumides toimuva tehnilise jälitustegevuse, objekti asukoha ja liikumise jälgimise, mis ei puuduta isikut ning võrguaadressi või lõppseadme identimisandmete hankimise (PaL 10. ptk § 13 lg 1, § 20 lg 2, § 22 lg 2 ja § 25 lg 3).

Piirangud tulenevalt sõnumiprivaatsusest

Sõnumi või muu teabe pealtkuulamist:

1) ei või rakendada kahtlustatava ja tema advokaadi (p 1), kahtlustatava ja vaimuliku vahel (p 2); kahtlustatava, kellelt on vabadus võetud, ja arsti, õe, psühholoogi või sotsiaaltöötaja vahelise suhtluse puhul (PaL 10. ptk §-s 52 lg 1);
2) ei või rakendada kergemate kuritegude puhul[110] ka suhtlusele kahtlustatava ja tema lähedase sugulase (p 1); kahtlustatava ja arsti, apteekri, ämmaemanda või sellise isiku assistendi (p 2); kahtlustatava ja avalikustatava teabe autori, avaldaja või meediateenuse osutaja vahel (p 3) (PaL 10. ptk § 52 lg 2).

Olukorras, kus ilmneb, et tegu on eelnimetatud vestlustega, tuleb lõpetata meetme rakendamine ning salvestised tuleb kohe hävitada (PaL 10. ptk § 52 lg 3). Erandiks on vestlused eelmainitud ametite esindajate ja sugulastega, kui ametite esindajaid või sugulasi kahtlustatakse sama kuriteo toimepanemises (PaL 10. ptk § 52 lg 4).

Teavitamine

Kriminaalmenetluses peab SUPO arvestama isiku õigusega meetmete kohta teavet saada (EL 4. ptk § 15 lg 5). Enamiku meetmete[111] kasutamise kohta tuleb kahtlustatavale esitada kirjalik teavitus hiljemalt aasta pärast seda, kui asi on saadetud prokurörile arutamiseks või kriminaalmenetlus on muul põhjusel lõpetatud või peatatud (PaL 10. ptk § 60 lg 1).

Kahtlustatavat tuleb põhjendamatu viivituseta või pärast asja saatmist prokurörile kirjalikult teavitada tema suhtes varjatud tegevuse, näilise tehingu või teabeallika kasutamisest (PaL 10. ptk § 60 lg 2). Kohus võib teavitamise edasi lükata kuni kahe aasta võrra, kui sellega kaitstakse teabekogumise või riigi turvalisust või elu ja tervist (PaL 10. ptk § 60 lg 3). Viivitamisel või teavitamata jätmisel peab asutus kaaluma kahtlustatava õigusi kriminaalmenetluses (PaL 10. ptk § 60 lg 6). Näilisest tehingust ja teabeallika kasutamisest teavitamise otsustab Helsinki Ringkonnakohus (PaL 10. ptk § 60 lg 7).

Teavitamise järel on isikul õigus saada teavet dokumentide või salvestiste kohta, kui nende avaldamata jätmine ei ole põhjendatud riigi turvalisuse, elu, tervise ja turvalisuse kaitse või taktikaliste, tehniliste protseduuridega, mida hoitakse salajasena. Teabe andmata jätmisest tuleb isikut teavitada (PaL 10. ptk § 62 lg 2).

Vahistamisõigusega ametnik võib olulisel menetluslikul põhjusel keelata kolmandal isikul avaldada teavet, mis on talle teatavaks saanud salajaste teabe kogumise meetmete kasutamise käigus. Teabe avaldamise õigust saab piirata, kui isik on teavet saanud ameti/ ülesande tõttu või olukorras, kus isikut

[110] Kergemad kuriteod, mille eest maksimaalne võimalik karistus on alla kuue aasta vangistust.

[111] Elektroonilise side pealtkuulamise; muul viisil, kui elektroonilise pealtkuulamisega teabe kogumise; elektroonilise side liikluse jälgimise; süstemaatilise jälituse; varjatud teabehanke; tehnilise seadme abil jälgimise; kontrollitud läbipääsu teostamise

on palutud appi meetme kasutamisel (PaL 10. ptk § 49 lg 1). Teabe avaldamise keeldu võib kohaldada kuni aastaks korraga ja keelust tuleb isikut teavitada kirjalikult.

5.3.2. PVTK

PVTK peab lähtuma kuritegude ennetamisel ja avastamisel samadest põhimõtetest nagu SUPO-gi: põhiõiguste austamine, proportsionaalsus, väikseima kahju põhimõte, eesmärgipärasuse põhimõte (LSRP § 88).

PVTK ametnikele kehtib Soome-vastase luuretegevuse ja sõjalise riigikaitse eesmärki ohustavate kuritegude ennetamisel ja avastamisel samad õigused ja piirangud, sh protseduurid meetmete kasutamiseks, mis SUPO-le (LSRP § 89 lg 1 esimene lause).

Eespool nimetatud meetmete rakendamine on lubatud PVTK-le vaid Soome-vastast luuretegevust hõlmavate riiklikku sõjalist kaitset ja tegevust ohustavate kuritegude paljastamisel (LSRP § 89 lg 2):

1) Soome enesemääramisõiguse ohustamine (p 1);
2) sõja õhutamine (p 2);
3) riigireetmine ja raske riigireetmine (p 3);
4) spionaaž ja raske spionaaž (p 4);
5) turvalisussaladuse paljastamine (p 5); ning
6) loata luuramine (välisriigi vastu Soome territooriumilt) (p 6).

Isikuandmete kaitse

PVTK peab lisaks eelnevale järgima isikuandmete kogumise ja säilitamise reegleid. Isikuandmeid võib koguda ja salvestada kaitseväeteenistuse õigusinfosüsteemi, turvateaberegistrisse, ajutistesse isikuregistritesse, distsiplinaarlahendite registrisse siis, kui andmete käitlemine on registri kasutuseesmärgi seisukohalt vajalik (LSRP § 121 lg 1). Isikuandmeid rassi või etnilise kuuluvuse, sotsiaalse, poliitilise või religioosse või ametiühingusse kuuluvuse, isiku tervist või ravi puudutavate küsimuste, seksuaaleluküsimuste või isiku sotsiaalabivajaduse ja saadavate toetuste kohta võib koguda ja salvestada eelnimetatud registritesse vaid siis, kui andmete käitlemine on kaitsejõudude pädevusse kuuluvate kuritegude lahendamise, ennetamise või avastamise ülesannete (LSRP §-de 7, 35, § 86 lõike 1) kohaldamisalasse kuuluva üksiku ülesande täitmiseks vältimatu (LSRP § 121 lg 2). Isikuandmeid isiku sooritatud kuriteo, karistuse või muu kriminaalsanktsiooni kohaldamise kohta võib koguda ja salvestada nimetatud isikuregistrisse siis, kui andmete käitlemine on andmesubjekti oma ohutuse või asutuse tööohutuse tagamiseks vältimatu (LSRP § 121 lg 3).

5.4. Järelevalve korraldus julgeoleku- ja luureasutuste tegevuse õigus- ja eesmärgipärasuse üle

(a) Teenistuslik järelevalve

SUPO tegevuse üle, sh salajaste teabe kogumise meetmete kasutamise üle kuritegude ennetamisel ja avastamisel, teostavad järelevalvet politseiasutuste juhid ja siseministeerium (PolS 5. ptk § 63 lg 1). Politsei salajaste teabe kogumise meetmete kasutamise üle kriminaalmenetluses teostavad järelevalvet samuti neid kasutavate üksuste juhid ning siseministeerium (PaL § 65 lg 1).

SUPO direktor peab hoidma siseministeeriumi informeerituna SUPO-t puudutavatest asjadest (LPH § 4a lg 2). Samuti peab SUPO teavitama tema ülesanneteks olevatest ühiskondlikult olulistest asjadest siseministrit ning lisaks politseipeadirektorit, kui neil asjadel on oluline mõju politsei muule tegevusele (LPH § 4a lg 1).

PVTK tegevuse üle teevad järelevalvet nii kaitsejõudude juhtkond kui ka luureosakonna ülem, kellel on oma pädevusala. Järelevalvet teeb kaitsejõudude juhtkond PVTK kuritegudega võitlemise osas ja luureosakonna ülem Soome vastu suunatud luuretegevuse ja sõjalise riigikaitse eesmärki ohustava tegevusega seotud kuritegude ennetamise ja avastamise üle (LSRP § 127).

PVTK üle teostab lisaks teenistuslikku järelevalvet Kaitseministeerium, sest PVTK kuulub Kaitseministeeriumi valitsemisalasse. Näiteks tuleb PVTK-l salajaste sunnivahendite ja salajaste teabe kogumise meetmete kasutamise kohta koostatud aruanne edastada Kaitseministeeriumile (LSRP § 128 lg 1). Lisaks peab PVTK teavitama Kaitseministeeriumi kaitsejõududes kuritegudega võitlemisega seotud asjaoludest, mis on ühiskondlikult, majanduslikult olulised või mis kujutavad tõsist ohtu (LSRP § 128 lg 2).

PVTK üle teostab järelevalvet ka SUPO. Nimelt on kaitsejõududes kuritegude ennetamise ja avastamisega tegeleja kohustatud ilma põhjendamatu viivituseta teatama salajaste teabe kogumise meetmete kasutamisest SUPO-le (LSRP § 89 lg 3).

Lisaks peab Kaitseministeerium SUPO-le esitama teadmiseks sama aruande, mille Kaitseministeerium esitab parlamendi ombudsmanile kord aastas salajaste sunnivahendite (LSRP §-s 37) ja salajaste teabe kogumise meetmete (LSRP § 89 lg 1) kasutamise, nende kaitsmise ja järelevalve kohta (LSRP § 129).

(b) Parlamendi ombudsmani järelevalve

Siseministeerium esitab parlamendi ombudsmanile korra aastas aruande SUPO kasutatud salajaste teabe kogumise meetmete ning nende kaitsmise ja järelevalve kohta kuritegude ennetamisel ja tõkestamisel ning lahendamisel (Pol 5. ptk § 63 lg 2, PaL 10. ptk § 65 lg 2). Sätted, mis reguleerivad aruandlust kuritegude tõkestamiseks ja lahendamiseks kasutatud meetmete kohta, tulenevad politseiseadusest (PoL 5. ptk § 63 lg 3). Kriminaaluurimises kasutatud meetmete aruandlust reguleerivad sunnimeetmete seaduse sätted (PaL 10. ptk § 65 lg 3).

Kaitseministeerium esitab kord aastas parlamendi ombudsmanile aruande PVTK kasutatud salajaste sunnivahendite (LSRP §-s 37) ja salajaste teabe kogumise meetmete (LSRP § 89 lg 1) ning nende kaitsmise ja järelevalve kohta. Aruanne esitatakse lisaks teadmiseks SUPO-le (LSRP § 129).

(c) Õiguskantsleri järelevalve

Õiguskantsleril on õigus teostada järelevalvet ametiasutuste, sh SUPO tegevuse seaduslikkuse üle (õiguskantsleri seadus § 3). Õiguskantsler teostab asutuste üle järelevalvet nii oma initsiatiivil kui ka isikute kaebuste alusel (õiguskantsleri seadus § 4). Õiguskantsler ei teosta järelevalvet Kaitseväe, sh PVTK üle.

(d) Parlamendi komiteede järelevalve

Parlamentaarsel tasandil tegelevad julgeolekuasutuste tegevuse ja sellega seotud õigusloomega põhiseaduslikkuse, halduse ja välisasjade komisjonid.[112] Parlamendi komisjonide järelevalveõiguse täpne ulatus ei ole samas selge.

5.5. Julgeoleku- ja luureasutuste volitused ja meetmed elektroonilise side jälgimisel ning andmete töötlemisel ja talletamisel

SUPO võib kasutada süütegude ennetamiseks ja tõkestamiseks või menetlemiseks järgmiseid elektroonilise side jälgimise ja andmete töötlemise ning talletamise meetmeid:

1) elektroonilise side pealtkuulamine (PoL 5. ptk § 5, PaL 10. ptk § 3 lg 2, eriti p-d 1–3, 11);
2) teabe kogumine muul moel, kui elektroonilise side pealtkuulamisega (PoL 5. ptk § 6 lg 1, PaL 10. ptk § 4);

[112] Olli J. Teirilä, Hanna J. Nykänen. The Public Dimension of Intelligence Culture: The Search for Support and Legitimacy.

3) elektroonilise sideliikluse jälgimine (PoL 5. ptk § 8, PaL 10. ptk § 6 lg 2 p 6);
4) elektroonilise side liikluse jälgimine võrguaadressi või lõppseadme suhtes omaniku nõusolekul (PoL 5. ptk § 9, PaL 10. ptk § 7);
5) tugijaama andmete kogumine (PoL 5. ptk § 11, PaL 10. ptk § 10);
6) tehnilise seire teostamine elektrooniliste seadmete üle (PoL 5. ptk § 23, PaL 10. ptk § 23);
7) võrguaadressi või lõppseadme identimisandmete hankimine (PoL 5. ptk § 25, PaL 10. ptk § 25).

Kriminaalmenetluses võib SUPO lisaks hankida võrguaadressi või lõppseadme identimisandmeid kahtlustatava või süüdimõistetuga kontakti saamiseks (PaL 10. ptk § 8). Elektroonilise side ettevõtjad on kohustatud asutust abistama, andma vajaliku ligipääsu ning pakkuma informatsiooni, seadmeid või personali toimingute teostamiseks (PaL 10. ptk § 63, Pol 5. ptk § 61).

Ühe kuriteo avastamisel või tõkestamisel või uurimisel kogutud teavet (nn üleliigset teavet) võib kasutada ka teise kuriteo avastamiseks või tõkestamiseks, kui selle kuriteo avastamiseks või tõkestamiseks on lubatud sellist meedet kasutada (PoL 5. ptk § 54, PaL 10. ptk § 56). Täiendavalt võib seda teavet kasutada teatud kuritegude uurimiseks, kui teave omab väga suurt tähtsust (PoL 5. ptk § 54 lg 2, PaL 10. ptk § 56 lg 2). Kasutamise tõendina otsustab asja lahendamisel kohus. Teavet võib kasutada alati kuriteo tõkestamiseks, politseioperatsioonide juhtimiseks ja süütuse tuvastamiseks (PoL 5. ptk § 54 lg 4, PaL 10. ptk § 56 lg 4). Teavet võib kasutada ka hoidmaks ära ohtu elule, tervisele või vabadusele, kahju varale või keskkonnale, samuti rahalise kahju ärahoidmiseks (PoL 5. ptk § 54 lg 5, PaL 10. ptk § 56 lg 5).

Eelnevalt nimetatud meetmetega kogutud teave tuleb viivitamata hävitada, kui selgub, et kogutud teave ei ole vajalik kuriteo avastamiseks, ärahoidmiseks või uurimiseks (PoL 5. ptk § 55) või asi on lahendatud (PaL 10. ptk § 57). Üleliigset informatsiooni võib siiski säilitada eelmises lõigus nimetatud juhtudel (registris) (PoL 5. ptk § 55 lg 2, PaL 10. ptk § 57). Teave, mida ei säilitada registris ega kriminaaluurimismaterjalides, tuleb viivitamatult hävitada (PoL 5. ptk § 55 lg 2). Pärast kriminaalmenetluse lõppemist tuleb teavet säilitada viis aastat (PaL 10. ptk § 57).

Kui selgub, et elektroonilise side pealtkuulamisel on kuulatud pealt kedagi teist, kui see, kelle jaoks luba anti, lõpetatakse pealtkuulamine koheselt ning kõik teave hävitatakse koheselt. Sama kehtib ka seadme tehnilise seire osas (PoL 5. ptk § 56, PaL 10. ptk § 58).

Kiireloomuliste juhtumite puhul, kus elektrooniliste andmete (sh sõnumi sisu) kogumine on toimunud vahistamisõigusega politseiametniku poolt, tuleb kõik teave viivitamatult hävitada, kui kohus hindab, et kõik eeltingimused meetme kasutamiseks ei olnud täidetud (PoL 5. ptk § 57, PaL 10. ptk § 59). Selliste andmete kasutamine on lubatud siiski, kui on täidetud üleliigse teabe kasutamise tingimused (PoL 5. ptk § 57, § 54, PaL 10. ptk § 59, § 56).

PVTK võib iseseisvalt kasutada elektroonilise side jälgimisel järgmisi meetmeid:

1) tugijaama andmete hankimine (LSRP § 89 lg 1 p 1);
2) elektroonilise side aadressi või elektroonilise side lõppseadme identimisandmete hankimine (LSRP § 89 lg 1 p 7).

Nende meetmete kasutamisel kehtivad kaitsejõudude kuritegude ennetamise ja avastamisega tegelevate ametnike suhtes samad volitused, mis SUPO-le tema ennetava ja avastava ülesande täitmisel politseiseaduse alusel (LSRP § 89 lg 1 esimene lause).

5.6. Järeldused läbivate üldpõhimõtete kohta julgeoleku- ja luureasutuste tegevuse reguleerimisel ning elluviimisel

Julgeolekuasutuste tegevust reguleerivad Soomes mitmed õigusaktid. Asutuste konkreetsed pädevuste piirid ja meetmed on seadustes täpsustatud erinevalt. Nii jätab politseihalduse seadus SUPO konkreetsed ülesanded avatuks ja nende täpsustamine on jäetud vastavalt hetkeolukorrale siseministeeriumi reguleerida seadusest madalama õigusaktiga. Samas on SUPO volitused ja meetmed

kriminaalmenetluses ning väljaspool kriminaalmenetlust (kuritegude avastamiseks ja ennetamiseks), reguleeritud väga üksikasjalikult. PVTK sõjalist luuretegevust välisriikide vastu samas Soome seadusandlus ei reguleeri. Seda tegevust juhitakse asutusesiseste korralduste ja Kaitsejõudude suunistega.[113]

Julgeolekuasutuste kasutatavaid meetmeid reguleerivad seadused ühtlustati 2014. aastal toimunud reformi käigus. Nii on politseiseaduses ja sunnimeetmete seaduses sisuliselt samad meetmete loetelud (PoL 5. ptk, PaL 10. ptk). Erinevus seisneb üksnes seaduste rakendumisalades, mis on määratud tegevusvaldkondadega – kuritegude ennetamine ja avastamine ning nende lahendamine kriminaalmenetluses.[114]

Soome regulatsioon sätestab erinevad meetmed ning protseduurid (*ex ante* kui ka *ex post* järelevalvemehhanismid) põhiõiguste riive õiguspärasuse tagamiseks. Regulatsioonist nähtub, et julgeoleku tagamisel ning muude julgeolekuasutuste ülesannete täitmisel on lubatud kasutada erinevaid meetmeid, mis piiravad isikute põhiõigusi. Samas näeb regulatsioon ette mitmed üldpõhimõtted, nt proportsionaalsuse põhimõte, eesmärgipärasus, väikseima kahju põhimõte, ja tagatised, et isikute põhiõiguseid ei riivataks rohkem kui vajalik. Iga meetme puhul on piiritletud selgelt, milliste kuritegude ringi puhul on neid lubatud kasutada. Oluliseks põhiõiguste kaitse tagatiseks on Soome süsteemis see, et enamuse salajase teabe kogumise meetmete kasutamiseks on vajalik kohtu luba. Seega on põhiõiguste kaitse julgeolekuasutuste tegevuses väga olulisel kohal.

5.7. Soome ja Eesti regulatsioonide võrdlus

Nii Eesti kui ka Soome julgeoleku- ja luureasutuste tegevust reguleerivad mitmed õigusaktid. Samas on võrreldes Eestiga Soome regulatsioon olulisel määral ühtlustatud, mis puudutab eelkõige SUPO volitusi ja meetmeid kuritegude avastamiseks ja ennetamiseks ning kuritegu uurimiseks. Soome regulatsioon on sealjuures väga põhjalik ja täpne osas, millistel juhtudel milliseid meetmeid kasutada võib, erinevalt Eesti regulatsioonist. Teisest küljest ei reguleeri Soome õigusaktid PVTK luuretegevust välisriikide vastu, samal ajal kui Eestis on vastav regulatsioon nii Teabeameti kui ka Kaitseväe tegevuse osas seaduse tasemel reguleeritud.

Eesti ja Soome julgeoleku- ja luureasutuste süsteem on suhteliselt sarnased. Peamine sarnasus seisneb selles, et mõlemas riigis on julgeolekuasutuseks kaitsepolitsei, kes täidab julgeoleku tagamiseks nii korrakaitselisi, süütegude menetlemise kui ka vastuluure ülesandeid. Seega ei ole nii Eestis kui ka Soomes luureasutused eraldatud politseiasutustest. Samuti täidab julgeoleku- ja luureasutuste ülesandeid Kaitsevägi. Erinevuseks on see, et Eestis on välisteabe kogumiseks olemas eraldi asutus – Teabeamet.

Julgeoleku- ja luureasutuste ülesanded, volitused ja meetmed on üldises plaanis sarnased. Erinevusena saab välja tuua selle, et Soome õigusaktides on oluliselt täpsemalt määratletud kaitsepolitsei meetmed elektroonilise side ja elektrooniliste seadmete jälgimise jaoks. Samuti näeb Soome regulatsioon ette võimaluse teostada näilikke tehinguid ning lubada kontrollitud läbipääsu. Kaitseväe luure osas on PVTK kasutuses oluliselt vähem meetmeid kui Kaitseväe või Teabeameti kasutuses. Samas ei ole PVTK sõjaline luuretegevus välisriikide seaduste tasemel reguleeritud ning seda tegevust juhitakse asutusesiseste korralduste ja Kaitsejõudude suunistega. Erinevalt Eesti regulatsioonist ei ole Soomes julgeolekukontrolli läbiviimisel lubatud teostada jälitustoiminguid ega salajasi teabe kogumise meetmeid. Samuti ei näe Soome õigus sõnaselgelt ette võimalust tegutseda väljaspool Soome territooriumi.

Põhiõiguste riive õiguspärasuse tagamiseks sätestatud protseduuride osas on sarnane see, et üldiselt on piiritletud, milliste kuritegude avastamiseks, tõkestamiseks ning uurimiseks on vastavaid meetmeid lubatud kasutada. Samuti sarnanevad Eesti ja Soome regulatsioon osas, et mõlemas regulatsioonis peavad julgeolekuasutused lähtuma oma tegevuses põhiõiguste kaitse, proportsionaalsuse ja eesmärgipärasuse põhimõtetest. Samas on Soome regulatsioon oluliselt detailsem, sätestades iga

[113] Ministry of Defence. Guidelines, lk 25 lg 4.
[114] Ministry of Defence. Guidelines, lk 13-14.

meetme puhul eraldi, milliste kuritegude tõkestamiseks ja millistel tingimustel meetme kasutamine lubatud on.

Oluline erinevus Eesti regulatsiooniga võrreldes seisneb selles, et Soomes on suurema osa salajase teabe kogumise meetmete kasutamiseks vaja kohtu luba ning et prokuratuurile ei ole antud sellist rolli nagu Eestis. Seega võib võrreldes Eestiga pidada Soomes tugevamaks *ex ante* kontrolli. Kohtu luba on Soomes näiteks vajalik elektroonilise side liiklusandmete (meta-andmete) jälgimiseks. Eestis võib see toimuda kas asutuse juhi või volitatud ametniku loal, prokuratuuri loal või ilma eelneva loamehhanismita (sõltuvalt sellest, millise seaduse alusel seda meedet kasutatakse). Soome kriminaalmenetluses on eluruumide salajase pealtkuulamise otsustamise menetluses lisaks erisus, mille kohaselt peab kohus menetluses määrama kahtlustatavale (pealtkuulatavale) riikliku esindaja, kelle ülesanne on kaitsta selle isiku õigusi.

Soome regulatsioon näeb samuti reeglina ette isiku teavitamise, kuid sellest nähakse ette mitmeid erandeid. *Ex post* järelevalvemehhanismide osas on sarnane teenistuslik järelevalve, samas Soomes teostab järelevalvet nii õiguskantsler kui ka parlamendi ombudsman. Erinev on ka see, et Eestis on oluline roll Riigikogu julgeolekuasutuste järelevalve komisjonil, kuid Soome parlamendi komisjonidele, mis tegelevad julgeoleku teemadega (nt halduskomisjon), ei ole antud selget volitust julgeolekuasutuste üle järelevalve teostamiseks.

Kokkuvõttes järgivad nii Eesti kui ka Soome regulatsioon sarnaseid üldisemaid põhimõtteid. Julgeolekuasutuste ülesannete täitmisel võib kasutada erinevaid meetmeid, mis piiravad isikute põhiõiguseid. Samas näevad mõlema riigi regulatsioonid ette sarnased põhimõtted (proportsionaalsuse põhimõte) ning erinevad kontrollimehhanismid (tagatised) põhiõiguste kaitseks.

6. ÜHENDKUNINGRIIK

6.1. Julgeoleku- ja luureasutused ning nende tegevust reguleerivad õigusaktid

Ühendkuningriigis on kolm julgeoleku- ja luureasutust:

1) **MI5 ehk Julgeolekuteenistus** (*Security Service*) on Ühendkuningriigi Siseministeeriumi haldusalasse kuuluv vastuluureteenistus (edaspidi: *MI5*);
2) **MI6 ehk Salaluureteenistus** (*Secret Intelligence Service*) on välisluureteenistus Ühendkuningriigi Välisministeeriumi haldusalas (edaspidi: MI6);
3) **Valitsusside Peakorter** (*Government Communications Headquarters* (GCHQ)) on Ühendkuningriigi signaalluureasutus. Asutus allub koos Salaluureteenistuse MI6'ga Ühendkuningriigi Välisministeeriumile ja selle allüksused, mis asuvad väljaspool Ühendkuningriigi territooriumi (Gibraltar, Türgi, Omaan, Küpros) asuvates Ühendkuningriigi sõjaväebaasides, alluvad Kaitseministeeriumile.

Ühendkuningriigis on kolm peamist õigusakti, mis reguleerivad julgeoleku- ja luureasutuste tegevust. *Security Service Act* 1989 ehk julgeolekuteenistuse seadus (edaspidi: SSA) sätestab Julgeolekuteenistuse ehk MI5 õigusliku aluse, reguleerides MI5 funktsioone ning määratledes, milliste ja mis ulatusega ohtudega MI5 tegelema peab.

Intelligence Services Act 1994 ehk luureteenistuse seadus (edaspidi: ISA) reguleerib Salaluureteenistuse ehk MI6 ja Valitsusside peakorteri funktsioone ja ülesandeid.

Regulation of Investigatory Powers Act 2000 ehk uurimisvolituste seadus (edaspidi: RIPA) sätestab julgeoleku- ja luureasutuste kasutatavate meetmete õigusliku raamistiku ning järelevalve nende tegevuse üle.

Lisaks nendele seadustele on üksikud julgeoleku- ja luureasutuste tegevust reguleerivad sätted ka järgnevates seadustes:

1) *Data Retention and Investigatory Powers Act* 2014 ehk andmete säilitamise ja uurimisvolituste seadus (edaspidi: DRIPA);
2) *Telecommunications Act* 1984 ehk telekommunikatsiooniseadus (edaspidi: TCA);
3) *Justice and Security Act* 2013 ehk õigluse ja julgeoleku seadus (edaspidi: JSA).

Samuti on teatud julgeoleku- ja luureasutuste volituste ja meetmete kohta välja antud tegevusjuhised (*code of practice*). Nende tegevusjuhiste eesmärk on anda julgeoleku- ja luureasutustele juhiseid, kas ja millistel tingimustel võib meetmeid kasutada ning mis protseduure tuleb meetmete kasutamisel järgida. Juhistes on kokkuvõtvalt välja toodud kõik meedet puudutavad õigusaktide sätted koos põhjalike selgitustega (koos näidetega). Need juhised on järgmised:

1) *Code of practice for the investigation of protected electronic information* ehk krüpteeritud elektroonilise informatsiooni uurimise tegevusjuhis;
2) *Covert human intelligence sources code of practice* ehk varjatud inimluure allikate kasutamise tegevusjuhis;
3) *Covert surveillance and property interference code of practice* ehk varjatud jälitustegevuse ja omandisse sekkumise tegevusjuhis;
4) *Code of practice for the acquisition and disclosure of communications data* ehk sideandmete hankimise ja edastamise tegevusjuhis;
5) *Code of practice for the retention of communications data* ehk sideandmete säilitamise tegevusjuhis;
6) *Equipment Interference Code of Practice* ehk seadmesse sekkumise tegevusjuhis;
7) *Interception of communications code of practice* ehk side pealtkuulamise tegevusjuhis.

Lisaks tegevusjuhistele on luure- ja julgeolekuasutusele siduvad korraldused, mis reguleerivad massilist andmete kogumist ja massilist sideandmete kogumist. Need korraldused on järgmised:

1) *Arrangements for the Acquisition of Bulk Communications Data Pursuant to Directions under Section 94 of the Telecommunications Act* 1984 ehk korraldus massilise sideandmete kogumise kohta vastavalt telekommunikatsiooniseaduse artiklile 94.
2) *Arrangements under section 2(2)(a) of the Security Service Act 1989 and sections 2(2)(a) and 4(2)(a) of the Intelligence Services Act 1994 for the obtaining and disclosing of bulk personal datasets* ehk korraldus massilise andmete kogumise ja edastamise kohta vastavalt julgeolekuteenistuse seaduse artiklile 2(2)(a) ja luureteenistuse seaduse artiklile 4(2)(a).

16.11.2016 võeti vastu uus *Investigatory Powers Act* ehk uurimisvolituste seadus, mis ühtlustab massiliste andmete ning massiliste sideandmete kogumise protseduure ning seab selged alused, millistel juhtudel võib nende meetmete kasutamiseks luba taotleda ning mida peab jälgima loa andmisel. Lisaks reguleerib seadus täpsemalt järelevalve teostamist nimetatud meetmete kasutamise üle. Kuna tegemist ei ole veel[115] jõustunud õigusaktiga, ei käsitle käesolev analüüs nimetatud õigusakti.

6.2. Julgeoleku- ja luureasutuste ülesanded, volitused ja meetmed põhiõiguste piiramisel

MI5 ehk Julgeolekuteenistuse ülesanded on SSA kohaselt järgmised:

1) rahvusliku julgeoleku kaitsmine ning eriti rahvusliku julgeoleku kaitsmine ohtude eest, mis tulenevad spionaažist, terrorismist ja sabotaažist, ohtude eest, mis tulenevad võõrvõimude agentide tegevusest ning ohtude eest, mis tulenevad tegevustest, mille eesmärk on parlamentaarse demokraatia kukutamine või õõnestamine poliitilisel, tööstuslikul või vägivaldsel teel (SSA § 1 lg 2);
2) Ühendkuningriigi majandusliku heaolu kaitsmine ohtude vastu, mis tulenevad välisriikides asuvate isikute kavatsustest või tegudest (SSA § 1 lg 3);
3) politseijõudude ning muude õiguskaitseorganite toetamine nende tegevuses raskete kuritegevuse ennetamisel ja avastamisel (SSA § 1 lg 4).

MI6 ehk Salaluureteenistuse ülesanded on ISA kohaselt järgmised:

1) välisriikides asuvate isikute tegude ning kavatsuste kohta informatsiooni hankimine ja edastamine (ISA § 1 lg 1 p (a));
2) teiste ülesannete täitmine välisriikides asuvate isikute tegude ja kavatsuste suhtes (ISA § 1 lg 1 p (b)).

Seejuures peab MI6 nimetatud ülesandeid täitma vaid (ISA § 1 lg 2):

1) rahvusliku julgeoleku huvides, eriti küsimustes, mis on puutumuses valitsuse kaitse- ja välispoliitikaga;
2) Ühendkuningriigi majandusliku heaolu huvides;
3) raskete kuritegude ennetamise ja avastamise toetamiseks.

Valitsusside Peakorteri ülesanded on ISA kohaselt järgmised:

1) elektromagnetiliste, akustiliste ning muude kiirguste ja neid kiirgusi tekitavate seadmete jälgimine ning nendesse sekkumine ning sellistest kiirgustest, seadmetest või dekrüpteeritud materjalist saadud või nendega seotud informatsiooni kogumine ja edastamine (ISA § 3 lg 1 p (a));
2) nõu ning abi andmine Briti relvajõududele, valitsusele või muudele asutustele seoses: (i) keeltega, sealhulgas terminoloogiaga, mida kasutatakse tehnilistes küsimustes, (ii) krüptograafiaga ning muude teemadega, mis seonduvad informatsiooni ja muude materjalide kaitsmisega (ISA § 3 lg 1 p (b));

Seejuures peab Valitsusside Peakorter nimetatud ülesandeid täitma vaid (ISA§ 2 lg 2):

[115] St uuringu koostamise ajal (s.o. november 2016).

1) rahvusliku julgeoleku huvides, eriti küsimustes, mis on puutumuses valitsuse kaitse- ja välispoliitikaga;
2) Ühendkuningriigi majandusliku heaolu huvides;
3) raskete kuritegude ennetamise ja avastamise toetamiseks.

Nii MI5, MI6 kui ka Valitsusside Peakorteril on oma ülesannete täitmiseks volitus andmeid koguda ja töödelda, sealjuures sekkuda isikute sõnumisaladusse ning kodu, perekonna- või eraellu. MI6 ning Valitsusside Peakorteril on volitus tegutseda ka välisriikides (teostada jälitustegevust).

Järgnevalt kirjeldatakse meetmeid, mida kasutavad nii MI5, MI6 kui ka Valitsusside Peakorter. Erandina võivad välisriikides viia läbi jälitustegevust üksnes MI6 ja Valitsusside Peakorter. Meetmeid reguleerib suures ulatuses RIPA selle erandiga, et välisriikides läbiviidud jälitustegevust ja seadmesse sekkumist reguleerib ISA, massilist andmete kogumist reguleerivad ISA ja SSA ning massilist sideandmete kogumist TCA.

Luure- ja julgeolekuasutused võivad oma ülesannete täitmisel kasutada järgmiseid meetmeid:

1) pealtkuulamine[116] (RIPA § 1);
2) sideandmete hankimine[117] (RIPA § 21 lg 1);
3) varjatud inimluure allikate kasutamine[118] (RIPA § 26 lg 1 p (c));
4) suunatud jälitustegevus[119] (RIPA § 26 lg 1 p (a));
5) sekkuv jälitustegevus[120] (RIPA § 26 lg 1 p (b));
6) krüpteeritud elektrooniliste andmete uurimine[121] (RIPA § 49);
7) jälitustegevus välisriikides[122] (ISA § 7);
8) seadmesse sekkumine[123] (ISA § 5);

---

[116] Pealtkuulamise (*interception*) all mõeldakse igasugust kommunikatsiooni pealtkuulamist kommunikatsiooni edastamise ajal kas avaliku postiteenuse või eratelekommunikatsiooni süsteemi kaudu. Siia alla kuulub näiteks pealtkuulamisseadmete kasutamine telefonikõnede pealtkuulamiseks ning posti lugemine.

[117] Sideandmete kogumise (*acquisition and disclosure of communications data*) all mõeldakse sideandmete kogumist postiteenuse või telekommunikatsioonisüsteemi kaudu. Sideandmete alla kuulub informatsioon side kohta (nt telefoninumbrid), aga mitte kommunikatsiooni sisu ise (RIPA§ 21 lg 6). See eristab seda eelmises punktis sätestatud pealtkuulamisest, mille eesmärk on saada teada kommunikatsiooni sisu. Lisaks sellele võivad luure- ja julgeolekuasutused välja teatisi, millega kohustatakse posti- või kommunikatsioonioperaatorit: (i) sideandmete kogumiseks, kui operaatoril sideandmed puuduvad, ning (ii) avaldama kogu olemasoleva informatsiooni sideandmete kohta (RIPA § 22 lg 4).

[118] *use of covert human intelligence sources*: isik on varjatud inimluure allikas, kui ta loob või säilitab varjatult isiklikku või muud laadi suhet isikuga eesmärgiga saada informatsiooni või saada ligipääsu informatsioonile teise isiku kohta ning edastada sellist informatsiooni (RIPA § 26 lg 8).

[119] *directed surveillance*: jälitustegevus on suunatud, kui see pole sekkuv ja: (i) seda viiakse läbi seoses mingi spetsiifilise juurdluse või operatsiooni eesmärgiga (ii) sellisel viisil, et on tõenäoline, et tegevuse käigus saadakse isiku kohta isiklikku informatsiooni (RIPA § 26 lg 2).

[120] *intrusive surveillance*: sekkuvaks loetakse jälitustegevust siis, kui: (i) see viiakse läbi kellegi elamispinnal või erasõidukis ning (ii) kui tegevusse on kaasatud isik, kes viibib nimetatud kohtades või siis kasutatakse jälitusseadet (RIPA § 26 lg 3).

[121] Krüpteeritud elektroonilisteks andmeteks on andmed, mis on sattunud luure- või julgeolekuteenistuse kätte, teostades oma seadusjärget õigust pealtkuulamisele või oma õigust sideandmete hankimisele ja edastamisele (RIPA § 49 lg 1 p (b) ja (c)). Lisaks kuuluvad siia alla andmed, mis on luure- või julgeolekuasutus saanud muul seaduslikul viisil oma õigusi teostades (RIPA § 49 lg 1 p (e)).

[122] Seadus ei defineeri täpsemalt, mida mõeldakse jälitustegevuse all. ISA § 7 lg 3 sätestab vaid, et jälitustegevus peab olema läbi viidud vastava asutuse ülesannete täitmiseks. ISA § 7 lg 9 sätestab lisaks, et välisriikides läbiviidud tegevuse all mõeldakse ka igasugust tegevust, mis on küll läbi viidud Ühendkuningriigi territooriumil, aga mis on tehtud seoses seadmetega (*apparatus*) (sh igasugused elektroonilised seadmed, masinad, vahendid, juhtmed või kaablid) või ükskõik millega, mis tuleneb sellisest seadmest, mida usutakse olevat väljaspool Ühendkuningriigi territooriumit.

[123] Seadmesse sekkumise all mõeldakse: (i) luure- ja julgeolekueesmärkidel seadmest informatsiooni hankimist, (ii) informatsiooni hankimist seadme omaniku ja kasutuse kohta, (iii) riistvara- või tarkvara identifitseerimine,

9) massiline andmete kogumine ja säilitamine[124] (SSA § 2 lg 2, ISA § 2 lg 2 punkt (a), ISA § 4 lg 2 p (a));
10) massiline sideandmete kogumine ja säilitamine[125] (TCA § 94).

6.3. Protseduurid põhiõiguste riive õiguspärasuse tagamiseks

Põhiõiguse riive õiguspärasus on tagatud sellega, et meetmeid tohib kasutada ainult teatud julgeoleku kaitsega seotud juhtudel ning tegevus peab olema proportsionaalne ja vajalik. Regulatsioon näeb ette iga meetme puhul eraldi, millal loetakse meedet vajalikuks. Kui need tingimused pole täidetud, siis ei väljastata orderit ehk luba tegevuse läbiviimiseks. Õiguspärasuse tagamiseks on meetme puhul, mis on oma olemuselt pikka aega kestvad, sätestatud tähtaeg, kaua selle aluseks olev order kehtib. Kuivõrd suur osa meetmetest on reguleeritud RIPA-s, asuvad ka enamus põhiõiguste riive õiguspärasust tagavaid norme seal.

Õiguse pealtkuulamiseks annab minister (*Secretary of State*) orderi alusel (RIPA § 5 lg 1). Orderi võib erandjuhtudel anda välja ka MI5, MI6 või Valitsusside Peakorteri juhtival positsioonil isikud. Sellisteks erandjuhtudeks on:

1) kiireloomulised juhud, kui minister ise on selgelt andnud volituse selliselt orderi andmiseks;
2) juhud, kus order antakse eesmärgiga täita palvet, mis on esitatud kompetentse välisriigi organi poolt seoses riikidevahelise abistamiskokkuleppega ja kui tundub, et pealtkuulamise subjekt asub väljaspool Ühendkuningriiki ja pealtkuulamine toimub ainult seoses asukohtadega, mis jäävad väljapoole Ühendkuningriiki (RIPA § 7 lg 1 punkt (b) ja lg 2).

Pealtkuulamise jaoks võib minister orderi väljastada vaid juhul, kui orderi alusel läbiviidud tegevus on proportsionaalne, võrreldes eesmärgiga, mida tegevusega saavutada soovitakse (RIPA § 5 lg 2 ja 3). Lisaks peab orderi andmine olema vajalik. Vajalik on orderi andmine siis, kui tegevus, mida soovitakse teha, on:

1) rahvusliku julgeoleku huvides;
2) raskete kuritegude ennetamise ja avastamise toetamiseks;
3) Ühendkuningriigi majandusliku heaolu huvides;
4) eesmärgiga tagada riikidevahelise abistamiskokkuleppe jõustamist raskete kuritegude ennetamise ja avastamise toetamiseks.

Selleks, et hinnata, kas meede on vajalik ja proportsionaalne, tuleb võtta arvesse, kas meetmega saavutatavat eesmärki on mõistlikult võimalik saavutada ka muid meetmeid kasutades (RIPA § 5 lg 4).

---

eemaldamine, muutmine või asendamine eesmärgiga saada punktides (i) ja (ii) sätestatud informatsiooni., (iv) jälitustegevuse kergendamist seadme abil. Seadmesse sekkumine ei ole seaduses defineeritud, vaid tuleneb seadmesse sekkumise tegevusjuhisest (*Equipment Interference Code of Practice*) lk 7, p 1.6.

[124] Massiline andmete säilitamine ei ole seaduses defineeritud. Siiski on näiteks Luureasutuste Erivoliniku (*Intelligence Services Commissioner*) 2015. a aastaaruandes defineeritud seda kui andmekogu (*bulk personal dataset)* säilitamist, mis sisaldab personaalset informatsiooni paljude isikute kohta, kellest enamus ei ole luure- ja julgeolekuasutuste huviorbiidis. Need andmekogud on tihtipeale äärmiselt mahukad ning neid on võimatu manuaalselt töödelda, seega on need hoiustatud luure- ja julgeolekuasutuste analüütilistes süsteemides. Luure- ja julgeolekuasutused teostavad massilist andmete säilitamist üldiste normide alusel (SSA § 2 lg 2, ISA § 2 lg 2 punkt (a), ISA § 4 lg 2 p (a)), mis sätestavad nende kohustuse koguda ja väljastada informatsiooni ainult vajalikus ulatuses.

[125] Lisaks teatud subjektide kohta sideandmete kogumisele (vt eespool punkt b) toimub ka massiline sideandmete kogumine ja säilitamine. Ka seda pole seaduses defineeritud, kuid see on sarnane massilise andmete säilitamisega, ainuke erinevus on, et andmeteks on sideandmed. Punktis b) nimetatud sideandmete hankimisest erineb massiline sideandmete kogumine selle poolest, et punktis b) nimetatud sideandmete hankimise korral hangitakse sideandmed teatud isiku kohta ning neid sideandmeid saab kohe kasutada. Massilise sideandmete kogumise puhul aga kogutakse sideandmeid suurtesse andmebaasidesse, kuid andmetele pole piiramatut ligipääsu. Seega on andmed küll andmebaasides olemas, kuid nendele ligipääsemiseks ning andmebaasides otsingute läbiviimiseks on omad protseduurid, mida on reguleeritud allpool punktis 1.5.

Pealtkuulamiseks vajalik order on kehtiv kuus kuud, kui see on antud välja rahvusliku julgeoleku huvides või Ühendkuningriigi majandusliku heaolu huvides, muudel juhtudel on order kehtiv 3 kuud. Kui order on antud välja julgeolekuasutuse juhtival positsioonil isiku poolt, on see kehtiv 5 tööpäeva (RIPA § 9 lg 6).

Sideandmete hankimiseks annab loa MI5, MI6 või Valitsusside Peakorteri juht (RIPA § 22 lg 3). Asutuse juhil on õigus anda välja teatisi, millega kohustatakse posti- või kommunikatsioonioperaatorit:

1) sideandmete kogumiseks, kui operaatoril sideandmed puuduvad, ning
2) avaldama kogu olemasoleva informatsiooni sideandmete kohta (RIPA § 22 lg 4).

Kuigi sideandmete hankimine ja edastamine on reguleeritud RIPA-s, siis nende andmete säilitamist seadus ei reguleeri.

Sideandmeid võib hankida ja edastada vaid siis, kui see on vajalik. Vajalik on see siis, kui see on:

1) rahvusliku julgeoleku huvides;
2) raskete kuritegude ennetamise ja avastamise toetamiseks;
3) Ühendkuningriigi majandusliku heaolu huvides;
4) avaliku korra huvides;
5) rahvatervise huvides;
6) vajalik maksude või muu sarnase panuse, mis peab tasuma valitsusasutusele, hindamiseks või kogumiseks;
7) vajalik hädaolukorras isiku surma, kehavigastuse või füüsilise või vaimse tervise kahjustumise vältimiseks või vähendamiseks;
8) ükskõik millisel eelnevalt nimetamata põhjusel, mille määrab oma korraldusega minister (RIPA § 22 lg 1 ja 2).

Luba ning teatist ei tohi anda juhul, kui loa või teatise andmine ei ole proportsionaalne taotletava eesmärgiga (RIPA § 22 lg 5).

Varjatud inimluure allikate kasutamiseks annab loa MI5, MI6 või Valitsusside Peakorteri juht (RIPA § 29 lg 1, RIPA § 30 lg 4, RIPA lisa 1 lg 5 ja RIPA § 81 lg 1).

Varjatud inimluure allikate kasutamine peab olema proportsionaalne võrreldes eesmärgiga, mida tegevusega saavutada soovitakse. Lisaks peab see olema vajalik. Varjatud inimluure allikate kasutamine on vajalik, kui see on:

1) rahvusliku julgeoleku huvides;
2) raskete kuritegude ennetamise ja avastamise toetamiseks;
3) Ühendkuningriigi majandusliku heaolu huvides;
4) avaliku korra huvides;
5) rahvatervise huvides;
6) vajalik maksude või muu sarnase panuse, mis peab tasuma valitsusasutusele, hindamiseks või kogumiseks;
7) ükskõik millisel eelnevalt nimetamata põhjusel, mille määrab oma korraldusega minister (RIPA § 29 lg 2 ja 3).

Varjatud inimluure allikate kasutamiseks antud luba kehtib 12 kuud (RIPA § 43 lg 3 punkt (b)).

Suunatud jälitustegevuseks annab loa MI5, MI6 või Valitsusside Peakorteri juht (RIPA § 28 lg 1, RIPA § 30 lg 4, RIPA lisa 1 lg 5 ja RIPA § 81 lg 1). Volitust ei ole vaja, kui suunatud jälitustegevus toimub vahetu reaktsioonina mingile sündmusele või asjaolule, mille puhul ei oleks mõistlik volitust hakata taotlema (RIPA § 26 lg 2).

Suunatud jälitustegevus peab olema proportsionaalne võrreldes eesmärgiga, mida tegevusega saavutada soovitakse. Lisaks peab see olema vajalik. Suunatud jälitustegevus on vajalik, kui see on:

1) rahvusliku julgeoleku huvides;
2) raskete kuritegude ennetamise ja avastamise toetamiseks;
3) Ühendkuningriigi majandusliku heaolu huvides;
4) avaliku korra huvides;
5) rahvatervise huvides;
6) vajalik maksude või muu sarnase panuse, mis peab tasuma valitsusasutusele, hindamiseks või kogumiseks;
7) ükskõik millisel eelnevalt nimetamata põhjusel, mille määrab oma korraldusega minister (RIPA § 28 lg 2 ja 3).

Suunatud jälitustegevuse läbiviimiseks antud luba kehtib 3 kuud (RIPA § 43 lg 3 punkt (c)).

Sekkuvaks jälitustegevuseks annab orderi minister (RIPA § 32 lg 1, § 42 lg 1 ja § 81 lg 1 kohaselt).

Sekkuv jälitustegevus peab olema proportsionaalne võrreldes eesmärgiga, mida tegevusega saavutada soovitakse. Lisaks peab see olema vajalik. Sekkuv jälitustegevus on vajalik, kui see on:

1) rahvusliku julgeoleku huvides;
2) raskete kuritegude ennetamise ja avastamise toetamiseks;
3) Ühendkuningriigi majandusliku heaolu huvides (RIPA § 32 lg 2 ja 3).

Sekkuva jälitustegevuse läbiviimiseks antud order kehtib 6 kuud (RIPA § 44 lg 4 punkt (c)).

MI5, MI6 ja Valitsusside Peakorter võivad anda isikutele teatisi, millega kohustatakse isikut andma **krüpteeritud elektrooniliste andmete võtit**, kui on olemas eelnev kirjalik luba ministrilt (Lisa 2 § 3 lg 2).

Luure- või julgeolekuteenistus võib teatise andmisega nõuda võtme avaldamist isiku käest, kui luure- või julgeolekuteenistus usub, et krüpteeritud elektrooniliste andmete võti on isiku käes ning kui võtme avaldamine on:

1) rahvusliku julgeoleku huvides;
2) raskete kuritegude ennetamise ja avastamise toetamiseks;
3) Ühendkuningriigi majandusliku heaolu huvides;
4) vajalik julgeoleku- või luureasutuse seadusega sätestatud ülesande efektiivseks ja nõuetekohaseks täitmiseks;
5) proportsionaalne taotletava eesmärgiga;
6) vajalik seetõttu, et ilma teatise andmiseta võtme saamine mõistlikus vormis võimalik (RIPA § 49 lg 2).

Välisriigis jälitustegevuse läbiviimiseks saavad taotleda orderit MI6 ja Valitsusside Peakorter (ISA § 7 lg 3). Orderi võib välja anda minister või erakorralistel asjaoludel MI6 või Valitsusside Peakorteri juhtival positsioonil olev isik, kui minister ise on andnud selleks oma selge volituse (ISA § 7 lg 5). Seadus ei täpsusta, mis on nendeks erakorralisteks asjaoludeks.

Orderit jälitustegevuseks välisriigis tohib välja anda ainult siis, kui on tehtud vajalikud korraldused selleks, et tagada:

1) et välisriigis ei tehta ühtegi asja, mis ei ole vajalik MI6 või Valitsusside Peakorteri ülesannete korrektseks täitmiseks ja
2) et nende orderiga lubatud tegevused ja nende võimalikud tagajärjed oleks mõistlikud, võttes arvesse eesmärke, mida nende tegevustega saavutada üritatakse ja
3) et oleks tagatud piisavad korraldused selleks, et informatsiooni, mida tegevuste käigus saadakse ning mida tegevuse käigus avaldatakse, võib saada ning avaldada ainult ulatuses, mil see on vajalik ülesannete täitmiseks ning rahvusliku julgeoleku huvides, raskete kuritegude ennetamise ja avastamise toetamiseks ja kriminaalmenetluse eesmärkidel (ISA § 7 lg 3 punktid (b) ja (c)).

Ministri antud order kehtib 6 kuud ning juhtiva töötaja antud order kehtib 2 tööpäeva (kuivõrd see on antud erakorralistel juhtudel) (ISA § 7 lg 6). Minister tühistab orderi koheselt, kui ta arvab, et order ei ole enam vajalik (ISA § 8).

Seadmesse sekkumiseks peab orderi andma minister (ISA § 5 lg 2). Kui seadmesse sekkumise tulemusena saadakse isiku kohta privaatset informatsiooni, on vajalik ka suunatud jälitustegevuse luba või sekkuva jälitustegevuse order.

Minister võib orderi välja anda siis, kui (ISA § 5 lg 2):

1) see on vajalik luure- ja julgeolekuasutuste ülesannete täitmiseks;
2) kui see on proportsionaalne saavutatava eesmärgiga;
3) on tagatud piisavad korraldused selleks, et informatsiooni, mida tegevuste käigus saadakse ning mida tegevuse käigus avaldatakse, võib saada ning avaldada ainult ulatuses, mil see on vajalik ülesannete täitmiseks ning rahvusliku julgeoleku huvides, raskete kuritegude ennetamise ja avastamise toetamiseks ja kriminaalmenetluse eesmärkidel.

Order kehtib 6 kuud (ISA § 6 lg 2 p (a)). Kui minister leiab, et order pole enam vajalik, võib ta selle tühistada (ISA§ 6 lg 4).

Luure- ja julgeolekuasutused **koguvad ja säilitavad massiliselt andmeid** üldiste normide[126] alusel, mis sätestavad nende kohustuse koguda ja väljastada informatsiooni ainult vajalikus ulatuses[127].

Massiliste andmete kogumist reguleerib ka korraldus massiliste andmete kogumise kohta (*Arrangements under section 2(2)(a) of the Security Service Act 1989 and sections 2(2)(a) and 4(2)(a) of the Intelligence Services Act 1994 for the obtaining and disclosing of bulk personal datasets*[128]). Selle korralduse kohaselt käivad massiliste andmebaaside (*bulk personal datasets*) alla ka need andmebaasid, mis on kogutud teisi luure- ja julgeolekuasutuste meetmeid kasutades. Nii on massilisteks andmebaasideks ka andmebaasid, mis sisaldavad sekkuva ning suunatud jälitustegevuse käigus, varjatud inimluure allikaid kasutades ning ka seadmesse sekkumise käigus kogutud andmeid.[129]

Korralduse kohaselt võib massilisi andmeid koguda vaid siis, kui see on vajalik taotletava eesmärgi saavutamiseks, taotletava eesmärgiga proportsionaalne ning kui kogutakse ainult sellises ulatuses informatsiooni, nagu on vajalik[130].

Luure- ja julgeolekuasutustel on massiliste andmete kogumiseks ja andmebaaside kasutamiseks nähtud ette ka oma siseprotseduurid, kus on rangelt määratletud massiliste andmebaaside kogumiseks vajaliku loa saamise protseduur. Luba ei ole vaja, kui andmebaas on kogutud mingi muu meetme kasutamise käigus ning selle muu meetme kasutamisele on antud nõuetekohane luba (näiteks kui andmebaasi on andmeid kogutus sekkuva jälitustegevuse käigus) [131].

Seega pole enamasti massiliste andmete kogumiseks vaja ministri orderit ning vajalik on ainult luure- või julgeolekuasutuse juhi luba, mille andmist reguleerivad luure- või julgeolekuasutuse siseprotseduurid.[132]

---

[126] MI5 ja MI6 juhtidel on kohustus tagada, et MI5 ja MI6 koguvad ja väljastavad informatsiooni ainult ulatuses, mis on vajalik MI5 ja MI6 ülesannete täitmiseks ning ulatuses, milles see on vajalik (i) raskete kuritegude ennetamise ja avastamise toetamiseks (ii) ja kriminaalmenetluse eesmärkidel (SSA § 2 lg 2 punkt (a) ja ISA § 2 lg 2 punkt (a)). Valitsusside Peakorteri juhi kohustus on tagada, et Valitsusside Peakorteri kogub ja väljastab informatsiooni ainult ulatuses, mis on vajalik (i) Valitsusside Peakorteri ülesannete täitmiseks ning (ii) ulatuses, milles see on vajalik kriminaalmenetluse eesmärkidel (ISA § 4 lg 2 p (a)).

[127] Valitsuse Luure- ja Julgeolekukomisjoni 2015. a aruanne, lk 56, p 157. Kättesaadav Internetis: https://goo.gl/xQ500a

[128] Korraldus massilise andmete kogumise kohta. Kättesaadav: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473782/Handling_arrangements_for_Bulk_Personal_Datasets.pdf

[129] Vt eelmine, lk 2 p 2.9.

[130] Vt eelmine, lk 4 p 4.2.

[131] Vt eelmine, lk 5 p 4.6.

[132] Valitsuse Luure- ja Julgeolekukomisjoni 2015. a aruanne, lk 56, p 159. Kättesaadav: https://goo.gl/xQ500a

Nimetatud siseprotseduurid reguleerivad lisaks massiliste andmete kogumiseks loa andmisele ka massilistele andmebaasidele ligipääsu andmist.

Enne andmebaasile ligipääsu andmist ja otsingu läbiviimist läbitakse kolmeastmeline test, et otsustada, kas otsingu läbiviimine toimub legaalsel eesmärgil, on vajalik ja proportsionaalne. Seega kasutatakse andmebaase vaid siis, kui selleks on julgeolekukaalutlustel põhjus. Lisaks on andmebaasis otsingu läbiviimiseks vaja juhtival positsioonil oleva isiku luba. Mitte kõigil isikutel pole ligipääsu andmebaasidele. Isikud, kellele antakse ligipääs, läbivad eelnevalt koolituse, kus neile tutvustatakse seadusest tulenevaid kohustusi, proportsionaalsuse ja vajalikkuse nõuet ning seda, et iga otsingu kohta võib läbi viia auditi. Teatud andmebaasidele ligipääsuks (näiteks andmebaasid, mis sisaldavad informatsiooni religiooni, rassi, seksuaalse orientatsiooni jms kohta) läheb vaja veelgi rangemat koolitust.

Andmebaase säilitatakse vaid nii kaua, kui on vajalik. Igal julgeolekuasutusel on revisjonikomisjon, kes koguneb iga kuue kuu tagant, et vaadata üle andmebaasid, mis julgeolekuasutustel olemas on. MI5-l on iga andmebaasi ülevaatamiseks erinev periood, olenedes sellest, kui palju need privaatsusesse tungivad ning ärisaladusi sisaldavad. Kõrge riskiga andmebaase vaadatakse läbi iga 6 kuu tagant, keskmise riskiga iga 12 kuu tagant ning madala riskiga iga 2 aasta tagant. Andmebaasid, mille kohta leitakse, et neil ei ole enam operatiivset väärtust, kustutatakse. [133]

Siinkohal on oluline välja tuua, et 2016. aaasta juulis leidis Uurimisvolituste tribunal (*Investigatory Powers Tribunal*), et massiliste andmete kogumise režiimil ei olnud kuni 4. märtsini 2015 seaduslikku järelevalvet. 4. märtsil 2015 avaldati Valitsuse Luure- ja Julgeolekukomisjoni 2015 aruanne, millega seoses sätestati RIPA § 59 lg 1 alusel, et massiliste andmete kogumise ja säilitamise üle peab järelevalvet teostama Luureasutuste erivolinik (*Intelligence Service Commissioner*) [134].

Massiline sideandmete säilitamine ja kogumine. Minister võib oma teatisega kohustada telekommunikatsioonioperaatoreid kohustama säilitama sideandmeid, kui minister leiab, et see on vajalik (DRIPA § 1 lg 1). Vajalik on see järgmistel juhtudel:

1) rahvusliku julgeoleku huvides;
2) raskete kuritegude ennetamise ja avastamise toetamiseks;
3) Ühendkuningriigi majandusliku heaolu huvides;
4) avaliku korra huvides;
5) rahvatervise huvides;
6) vajalik maksude või muu sarnase panuse, mis peab tasuma valitsusasutusele, hindamiseks või kogumiseks;
7) vajalik hädaolukorras isiku surma, kehavigastuse või füüsilise või vaimse tervise kahjustumise vältimiseks või vähendamiseks;
8) ükskõik millisel eelnevalt nimetamata põhjusel, mille määrab oma korraldusega minister (DRIPA § 1 lg 1, RIPA § 22 lg 2).

Lisaks on teatise andmise eeldused sätestatud ka tegevusjuhises sellisel viisil sideandmete saamise ja säilitamise kohta (*Retention of Communications Data- Code of Practice*).

Seega on volitus sideandmete säilitamise kohustamiseks ainult ministril ning luure- ja julgeolekuasutused ei saa sellist kohustust telekommunikatsioonioperaatoritele panna.

Sideandmete edastamine telekommunikatsioonioperaatorite poolt. Telekommunikatsiooni-operaatorite kohustust sideandmeid luure- ja julgeolekuasutustele edastada reguleerib TCA. Selle seaduse § 94 sätestab üldsõnaliselt, et ministril on õigus kohustada telekommunikatsioonioperaatoreid "midagi tegema või millegi tegemisest hoiduma". Selle alusel on kohustatud

[133] Valitsuse Luure- ja Julgeolekukomisjoni 2015. a aruanne, lk 57-58, p 161-163. Kättesaadav: https://goo.gl/xQ500a

[134] Uurimisvolituste tribunali otsus, p 100 ja 101. Kättesaadav: https://www.documentcloud.org/documents/3143963-investigatory-powers-tribunal-bulk-data-judgment.html

telekommunikatsioonioperaatoreid edastama luure- ja julgeolekuasutustele regulaarselt sideandmeid[135]. Seega ei saa luure- ja julgeolekuasutused ise kohustada telekommunikatsioonioperaatoreid massilisi sideandmeid edastama, kuid seda tehakse praktikas ministri antud käsu alusel.

2015. a novembris võeti vastu luure- ja julgeolekuasutustele siduv korraldus, mis reguleerib TCA § 94 alusel sideandmete hankimist[136] (*Arrangements for the Acquisition of Bulk Communications Data Pursuant to Directions under Section 94 of the Telecommunications Act 1984*). Selle korralduse kohaselt võib minister kohustada telekommunikatsioonioperaatoreid edastama luure- ja julgeolekuasutustele sideandmeid ainult siis, kui see on vajalik, proportsionaalne ning kui pole ühtegi vähem riivavat meedet ning kui eelnevalt kaalutakse tagajärgi, mis kaasnevad eraellu tungimisega[137].

Kogutavad sideandmed jagunevad:

1) andmeliikluse andmed (*traffic data*) – andmed selle kohta, kes on saaja ning saatja; saatmise aeg ja koht ning muud sõnumi edastamise faktiga seotud andmed;
2) teenuse kasutamise informatsioon (*service use information*) – andmed teenuse kasutamise kohta, näiteks andmed, mis on tavaliselt kajastatud arvel, mis esitatakse isikule teenuste kasutamise eest;
3) tellijateave (*subscriber information*) – andmed, mida teenusepakkuja saab siis, kui teenuse tarbija teenust tellima hakkab, näiteks teenuse tellija nimi, aadress, telefoninumber, e-posti aadress[138].

2016. aasta juulis avaldas Sideandmete Jälgimise Erivolinik (*Interception of Communications Commissioner*) raporti, kus analüüsiti TCA § 94 alusel välja antud ministri käske. Selle kohaselt on Ühendkuningriigis juuli 2016 seisuga välja antud 15 ministri käsku, mille alusel kogutakse sideandmeid[139].

6.4. Järelevalve korraldus julgeoleku- ja luureasutuste tegevuse õigus- ja eesmärgipärasuse üle

(a) Luureasutuste Erivolinik

Luureasutuste tegevuste ning neile pandud õiguste ja kohustuste üle teostab järelevalvet Luureasutuste Erivolinik (*Intelligence Service Commissioner*, edaspidi Erivolinik) (RIPA § 59 lg 2 p (c)). Luureasutuste Erivoliniku ülesandeid seadus kitsamalt ei täpsusta. Luureasutuste Erivoliniku koduleheküljel on kirjeldatud, kuidas Erivolinik oma ülesandeid täidab.[140] Inspektsioonide käigus teostab Erivolinik kontrolli selle üle, kas sekkuva ning suunatud jälitustegevuse, välisriikides teostatava jälitustegevuse, seadmesse sekkumise, krüpteeritud elektrooniliste andmete uurimise, varjatud inimluure allikate kasutamise ning massiliste andmete kasutamise orderid on antud seaduse kohaselt. Seda teeb ta kolmes astmes.

Esimene aste on eellugemine. Luure- ning julgeolekuasutused esitavad Erivolinikule eellugemiseks nimekirja kõigist antud orderitest ning Erivolinik valib nende seast teatud arvu ordereid, mida ta uurib

[135]MTÜ Privacy International ülevaade julgeolekuasutuste meetmetest. Kättesaadav Internetis: https://www.privacyinternational.org/node/902
[136]Kättesaadav Internetis: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473780/Handling_arrangements_for_Bulk_Communications_Data.pdf
[137]Korralduse lk 4, p 4.1.1. Kättesaadav internetis: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473780/Handling_arrangements_for_Bulk_Communications_Data.pdf
[138] Vt eelmine, lk 21, punkt 8.3.
[139] Sideandmete Jälgimise Erivoliniku raport TCA § 94 alusel välja antud ministri käskude kohta, lk 20 punkt 7.4. Kättesaadav Internetis: http://www.iocco-uk.info/docs/56208%20HC33%20WEB.pdf
[140] Luureasutuste Erivoliniku koduleheküg. Kättesaadav Internetis: http://intelligencecommissioner.com/content.asp?id=5

koos kaasaskäiva dokumentatsiooniga. Nimekiri sisaldab ka väikest tutvustust selle kohta, mis asjaoludel on order antud. Lisaks valitakse mõned orderid kontrolliks välja juhuslikult.

Erivolinik vaatab orderid ning nendega seonduvad dokumendid põhjalikult läbi ning otsustab, kas tal läheb vaja lisainformatsiooni. Ta teeb kindlaks, kas orderi andmisel on piisavalt järgitud proportsionaalsuse ja vajalikkuse põhimõtteid ning kas privaatsusesse tungimine on põhjendatud. Selleks uurib ta, kas:

1) tegevus käib luure- või julgeolekuasutuse ülesannete alla;
2) tegevus oli vajalik: (a) rahvusliku julgeoleku huvides, (b) raskete kuritegude ennetamise ja avastamise toetamiseks, (c) Ühendkuningriigi majandusliku heaolu huvides;
3) tegevus on proportsionaalne: (a) informatsiooni poleks saanud saada vähem koormavate meetmetega, (b) piirangud on seatud, (c) on kaalutud seonduvaid tagajärgi, mis kaasnevad eraellu tungimisega.

Lisaks proportsionaalsusele kontrollib Erivolinik, kas informatsioon, mida kogutakse, on õigustatud võrreldes privaatsusega, millesse tungitakse ning kas tegevusele on antud luba pädeva isiku poolt.

Teine aste on asutuse inspekteerimine. Erivolinik külastab asutust, kelle antud orderit ta kontrollis ning suhtleb isikutega, kes sellega seotud on. Ta küsitleb neid isikuid ning tutvub kaasuse asjaoludega, et otsustada, kas order on antud seaduslikult ning kas kogutud informatsioon on piisavalt oluline, et privaatsusesse sekkumist õigustada ning et kas on kasutatud kõige vähemkoormavat meedet.

Kolmas aste on külastused, mis pole ette planeeritud. Paljud orderid on antud nii, et neis on tagatised, mis peaksid tagama võimalikult piiratud privaatsusesse sekkumise. Nende külastuste eesmärk on dokumentide uurimisest kaugemale minna ning vaadata, kuidas neid tagatisi tegelikkuses ellu viiakse. Erivolinik küsitleb luure- ja julgeolekuasutuste ametnikke erinevate operatsioonide eri staadiumites, et aru saada, kas neid tagatisi järgitakse.

Pärast kolmeastmelise järelevalve läbiviimist avaldab erivolinik oma leidude kohta raporti.

Alates aastast 2010 on Luureasutuste Erivolinikul järelevalve kohustus vaadata üle asutuste massiliste andmete andmebaase. See kohustus ei ole sätestatud seaduses. Erivolinik teostab kontrolli tagasiulatuvalt iga kuue kuu tagant. Järelevalve käigus vaatab ta, millised on julgeolekukaalutlused andmebaaside säilitamiseks, kas vajalikkuse ja proportsionaalsuse nõuded on täidetud ning kas esineb andmete väärkasutamist ja kuidas seda ennetatakse.[141]

(b) *Uurimisvolituste tribunal*

Uurimisvolituste tribunalil (*Investigatory Powers Tribunal*) on jurisdiktsioon lahendada vaidlusi, mis on esitatud luure- ja julgeolekuasutuste vastu. Kui tribunal lahendab vaide kaebaja kasuks, saab tribunal kohustada luure- või julgeolekuasutust tühistama orderit või luba, mille alusel tegevust teostatakse või kohustada luure- või julgeolekuasutust hävitama kogu informatsiooni, mis on kogutud orderi alusel või mis on luure- või julgeolekuasutusel isiku kohta (RIPA § 67 lg 7).

(c) Valitsuse Luure- ja Julgeolekukomisjon

Parlamendi Luure- ja Julgeolekukomisjon (*The Intelligence and Security Committee of Parliament*) on loodud JSA alusel. Luure- ja Julgeolekukomisjonil on õigus teostada järelevalvet MI5, MI6 ja Valitususside Peakorteri kulutuste, halduse ja tegevuse üle (JSA § 2 lg 1). Oma järelevalve käigus kogutud informatsiooni kohta peab komisjon esitama iga-aastase raporti valitusele (JSA § 3 lg 1). Komisjonil on õigus saada kogu informatsiooni asutuste tegevuste kohta, sealhulgas salastatud materjali kohta, mis on seotud nende asutuste tegevustega, mida komisjon uurib (JSA Lisa 1 § 4). Informatsiooni ei pea asutused avaldama juhul, kui minister on niimoodi otsustanud. Minister võib otsustada, et informatsiooni ei pea avaldama, kui: (i) see on riikliku julgeoleku huvides või (ii) kui avaldatav

[141] Valitsuse Luure- ja Julgeolekukomisjoni 2015. a aruanne, lk 57, p 160. Kättesaadav Internetis: https://goo.gl/xQ500a

informatsioon võib viia selleni, et identifitseeritakse käimasoleva operatsiooni informatsiooniallikad või meetmed (JSA § 4 lg 4 ja § 5).

(d) Sideandmete jälgimise erivolinik

Sideandmete Jälgimise Erivolinik (*Interception of Communications Commissioner*) teostab järelevalvet sideandmete hankimisel ja edastamisel sätestatud õiguste ja kohustuste täitmise üle (RIPA § 57 lg 2 p (b)). Sideandmete jälgimise erivolinik peab esitama peaministrile raporti järelevalve kohta pärast aasta lõppu esimesel võimalusel (RIPA § 58 lg 4).

6.5. Julgeoleku- ja luureasutuste volitused ja meetmed elektroonilise side jälgimisel ning andmete töötlemisel ja talletamisel

Elektroonilise side jälgimise ning andmete töötlemise ja talletamise regulatsioon on Ühendkuningriigis reguleeritud mitmes erinevas seaduses. Järgnevalt tuuakse välja erinevad meetmed elektroonilise side jälgimisel, andmete töötlemisel ja talletamisel. Protseduure nende meetmete kasutamisel põhiõiguste riive õiguspärasuse tagamiseks, samuti järelevalve mehhanisme on käsitletud eelmistes peatükkides.

(a) Sideandmete massiline kogumine ja töötlemine

Ühendkuningriigis hõlmab sideandmete kogumine järgmiseid andmeid:

1) andmeliikluse andmed (*traffic data*) – andmed selle kohta, kes on saaja ning saatja, saatmise aeg ja koht ning muud sõnumi edastamise faktiga seotud andmed;
2) teenuse kasutamise informatsioon (*service use information*) – andmed teenuse kasutamise kohta, näiteks andmed, mis on tavaliselt kajastatud arvel, mis esitatakse isikule teenuste kasutamise eest;
3) tellijateave (*subscriber information*) – andmed, mida teenusepakkuja saab siis, kui teenuse tarbija teenust tellima hakkab, näiteks teenuse tellija nimi, aadress, telefoninumber, e-posti aadress[142].

Seadus ei reguleeri, kuidas peab kogutud massilisi sideandmeid säilitama ning kellel ja mis tingimustel on ligipääs andmebaasidele, kus säilitatakse massilisi sideandmeid. Siiski on Valitsuse Luure- ja Julgeolekukomisjoni poolt koostatud raportis[143] välja toodud, et sideandmete säilitamine ja kasutamine on reguleeritud rangete sisereeglitega ja siseprotseduuridega. Lisaks on kehtestatud tegevusjuhis sellisel viisil kogutud sideandmete saamise ja säilitamise kohta (*Retention of Communications Data- Code of Practice*).

Selle tegevusjuhise kohaselt säilitatakse andmebaase vaid nii kaua, kui on vajalik. Igal julgeolekuasutusel on revisjonikomisjon, kes koguneb iga kuue kuu tagant, et vaadata üle andmebaasid, mis julgeolekuasutustel olemas on. MI5-l on iga andmebaasi ülevaatamiseks erinev periood, olenedes sellest, kui palju need privaatsusesse tungivad ning ärisaladusi sisaldavad. Kõrge riskiga andmebaase vaadatakse läbi iga 6 kuu tagant, keskmise riskiga iga 12 kuu tagant ning madala riskiga iga 2 aasta tagant. Andmebaasid, mille kohta leitakse, et neil ei ole enam operatiivset väärtust, kustutatakse.

Enne andmebaasis otsingu läbiviimist läbitakse kolmeastmeline test, et otsustada, kas otsingu läbiviimine toimub legaalsel eesmärgil, on vajalik ja proportsionaalne. Seega kasutatakse andmebaase vaid siis, kui selleks on julgeoleku tagamise kaalutlus. Lisaks on andmebaasis otsingu läbiviimiseks vaja juhtival positsioonil oleva isiku luba. Mitte kõigil isikutel pole ligipääsu andmebaasidele. Isikud, kellele antakse ligipääs, läbivad eelnevalt koolituse, kus neile tutvustatakse neile seadusest tulenevaid kohustusi, proportsionaalsuse ja vajalikkuse nõuet ning seda, et iga otsingu kohta võib läbi viia auditi.

[142] Vt eelmine, lk 21, punkt 8.3.
[143] Valitsuse Luure- ja Julgeolekukomisjoni 2015. a aruanne. Kättesaadav Internetis: https://goo.gl/xQ500a

Teatud andmebaasidele ligipääsemiseks (näiteks andmebaasid, mis sisaldavad informatsiooni religiooni, rassi, seksuaalse orientatsiooni jms kohta) läheb vaja veelgi rangemat koolitust.[144]

(b) Spetsiifiliste subjektide sideandmete kogumine ja avaldamine

Lisaks eelnevalt on luure- ja julgeolekuasutustel loa alusel õigus telekommunikatsioonioperaatoritelt koguda spetsiifiliste subjektide sideandmeid (v.a sõnumi sisu kohta) (RIPA § 21 lg 1). Kuigi sideandmete hankimine ja edastamine on reguleeritud RIPA-s, siis nende andmete säilitamist seadus ei reguleeri. Sideandmete säilitamist reguleerib sideandmete säilitamise tegevusjuhis (*Code of practice for the retention of communications data*) (vt eelmises punktis).

(c) Pealtkuulamine

Julgeolekuasutustel on õigus pealt kuulata elektroonilist sidet, sh lugeda elektroonilise side kaudu edastatavate sõnumite sisu (RIPA § 1). Pealtkuulamisega kogutud andmete töötlemine ja talletamine on reguleeritud RIPA-s.

Pealtkuulamisega kogutud andmete kasutamisel on ministril kohustus tagada, et järgnevad aspektid oleks võimalikult piiratud: (a) isikute arv, kellele pealtkuulamisega kogutud andmed tehakse teatavaks või muud moodi kättesaadavaks, (b) ulatus, milles materjale avaldatakse või tehakse muud moodi kättesaadavaks, (c) ulatus, milles materjale kopeeritakse, (d) koopiate arv. Lisaks täpsustatakse, et nimetatud aspekte peab hoidma võimalikult miinimumi lähedal ulatuses, mis on vajalik autoriseeritud ülesannete täitmiseks (RIPA § 15 lg 2). Nimetatud aspektide piiramise kaitse eesmärk on tagatud, kui kõik pealtkuulamisega saadud materjalidest tehtud koopiad hävitatakse kohe, kui ei ole enam aluseid nende säilitamiseks seoses autoriseeritud ülesande täitmise vajalikkusega (RIPA § 15 lg 3). Tegevus on vajalik ülesande täitmiseks siis, kui see on vajalik:

1) rahvusliku julgeoleku huvides, raskete kuritegude ennetamise ja avastamise toetamiseks, Ühendkuningriigi majandusliku heaolu huvides või eesmärgiga tagada riikidevahelise abistamiskokkuleppe jõustamist raskete kuritegude ennetamise ja avastamise toetamiseks;
2) selleks, et ministril oleks lihtsam otsustada, kas anda välja ordereid;
3) sideandmete Jälgimise Erivoliniku või Uurimisvolituste Tribunali järelevalve teostamisega seotud ülesannete täitmiseks;
4) tagamaks, et kriminaalmenetlust läbiviival isikul on piisavalt informatsiooni ausa menetluse läbiviimiseks (RIPA § 15 lg 4).

(d) Seadmesse sekkumine

Seadmesse sekkumine (ISA § 5) on üks meetmetest elektroonilise side jälgimisel ning andmete töötlemisel ja talletamisel, sest seadmesse sekkumise käigus võidakse koguda elektroonilise side kohta informatsiooni.[145]

Seadmesse sekkumise all mõeldakse: (i) luure- ja julgeolekueesmärkidel seadmest informatsiooni hankimist, (ii) informatsiooni hankimist seadme omaniku ja kasutuse kohta, (iii) riistvara- või tarkvara identifitseerimine, eemaldamine, muutmine või asendamine eesmärgiga saada punktides (i) ja (ii) sätestatud informatsiooni, (iv) jälitustegevuse kergendamist seadme abil. Seadmesse sekkumine ei ole seaduses defineeritud, vaid tuleneb seadmesse sekkumise tegevusjuhisest[146].

(e) Krüpteeritud elektrooniliste andmete uurimine

Krüpteeritud elektroonilisteks andmeteks on andmed, mis on sattunud luure- või julgeolekuteenistuse kätte pealtkuulamise või sideandmete hankimise käigus krüpteeritud kujul (RIPA § 49 lg 1 p (b) ja (c)).

---

[144] Valitsuse Luure- ja Julgeolekukomisjoni 2015. a aruanne, lk 57-58, p 161-163. Kättesaadav Internetis: https://goo.gl/xQ500a

[145] Vt eelmine, lk 7, p 1.6.

[146] Equipment Interference Code of Practice, lk 7, p 1.6. Kättesaadav Internetis: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/496069/53693_CoP_Equipment_Interference_Accessible.pdf

Lisaks kuuluvad siia alla andmed, mille on luure- või julgeolekuasutus saanud muul seaduslikul viisil oma õigusi teostades (RIPA § 49 lg 1 p (e)).

6.6. Järeldused läbivate üldpõhimõtete kohta julgeoleku- ja luureasutuste tegevuse reguleerimisel ning elluviimisel

Ühendkuningriigi julgeoleku- ja luureasutuste tegevuse regulatsioon on suhteliselt üldsõnaline ning ei kirjelda täpselt tegevuste läbiviimise protseduure. Meetmete reguleerimisel on keskendutud pigem kirjeldustele, millistel üldistel eesmärkidel võib teatud meetmeid kasutada ning millal loetakse meetme kasutamist vajalikuks. Oluline roll lisaks seadustele on vastava regulatsiooni kohta koostatud juhistel.

Ühendkuningriigis on olnud tõsiseid probleeme massilise andmete, sh sideandmete kogumise regulatsiooniga. Uurimisvolituste tribunal otsustas 2016. aasta juulis, et massilisi andmeid on aastaid kogutud nii, et kogumise üle puudus seaduslik järelevalve. Seaduslik järelevalve sätestati alles 4. märtsil 2015, kui avaldati Valitsuse Luure- ja Julgeolekukomisjoni 2015 aruanne, millega seoses sätestati RIPA § 59 lg 1 alusel, et massiliste andmete kogumise ja säilitamise üle peab järelevalvet teostama Luureasutuste Erivolinik.[147]

Lisaks otsustas Uurimisvolituste tribunal samas otsuses, et massiliste sideandmete kogumise režiim oli kuni 4. novembrini 2015 ebaseaduslik. Nimelt võeti alles 4. novembril 2015 vastu korraldus, mis reguleerib TCA § 94 alusel sideandmete hankimist (*Arrangements for the Acquisition of Bulk Communications Data Pursuant to Directions under Section 94 of the Telecommunications Act 1984*). Enne seda puudus sideandmete kogumise kohta piisav regulatsioon.

Hetkel kehtivast regulatsioonist nähtub, et julgeoleku tagamisel ning muude julgeolekuasutuste ülesannete täitmisel on lubatud kasutada erinevaid meetmeid, millega riivatakse oluliselt inimeste põhiõigusi. Regulatsioon sätestab samas protseduurid (*ex ante* kui ka *ex post* järelevalvemehhanismid) põhiõiguste riive õiguspärasuse tagamiseks. Näiteks näeb regulatsioon ette, et erinevaid meetmeid võib kasutada üksnes siis, kui meede on proportsionaalne võrreldes eesmärgiga, mida tegevusega saavutada soovitakse, ning vajalik. Suurema osa meetmete kasutamine toimub ministri loa alusel. Euroopa Inimõiguste Kohtu hinnangul võib konventsiooniga olla kooskõlas olukord, kus loa pealkuulamiseks annab kohtuväline organ, kuid seda üksnes tingimusel, et see organ on sõltumatu täitevvõimust ning sellel organil piisavalt võimu ning pädevust teostada tõhusat ning pidevat kontrolli.[148] Euroopa Inimõiguste Kohus on olnud seisukohal, et igasugune poliitilise iseloomuga loa andmine ning jälgimine suurendab riski, et meetmeid kuritarvitatakse, mistõttu võib eeldada, et poliitiline isik nagu minister ei suuda anda piisavalt tagatisi.[149] Samas võib tugev kohtulik järelkontroll või muu kontroll tasakaalustada algse volituse andmise puudujääke.[150] Võttes arvesse meetmete kasutamise tingimusi üldiselt ning erinevate järelevalveorganite ning asutuste olemasolu ja pädevusi, on põhiõiguste kaitse julgeolekuasutuste tegevuse regulatsioonis väga olulisel kohal.

Probleeme on siiski seoses massiliste (side)andmete kogumisega. Seetõttu võeti 16.11.2016 vastu uus uurimisvolituste seadus (*Investigatory Powers Bill*)[151]. Kuningliku nõusoleku (*royal assent*) sai seadus 29.11.2016. Uus uurimisvolituste seadus ühtsustab massiliste (side)andmete kogumise režiimi ning seab selged alused, mis juhtudel võib luba taotleda ning milline on protseduur loa andmiseks. Lisaks reguleerib seadus järelevalvet andmete kogumise üle. Sõltumata selge õigusliku aluse sätestamisest, heidetakse sellele seadusele ette Ühendkuningriikide julgeoleku- ja luureasutustele kõige

[147] Uurimisvolituste tribunali otsus, p 100 ja 101. Kättesaadav: https://www.documentcloud.org/documents/3143963-investigatory-powers-tribunal-bulk-data-judgment.html
[148] *EIKo Szab and Vissy vs Hungary*,p 77. EIKo *Klass and others vs Germany*, p 56.
[149] *EIKo Szab and Vissy vs Hungary*,p 77.
[150] *EIKo Szab and Vissy vs Hungary*, p 77; EIKo *Kennedy*, p 167.
[151] Ühendkuningriigivalitsuse kodulehel asuv eelnõu: http://services.parliament.uk/bills/2015-16/investigatorypowers.html

laiaulatuslikumate volituste andmist nuhkimiseks ja andmete kogumiseks kui üheski teises Lääne-Euroopa riigis või USA-s.[152]

6.7. Ühendkuningriigi ja Eesti regulatsioonide võrdlus

Võrreldes Eestiga reguleerib Ühendkuningriigi julgeoleku- ja luureasutuste tegevust oluliselt väiksem hulk õigusakte. Erinevalt Eestist, reguleerivad Ühendkuningriigis julgeolekuasutuste kasutatavaid meetmeid ka tegevusjuhised, mille eesmärk on anda julgeoleku- ja luureasutustele juhiseid, kas ja millistel tingimustel võib meetmeid kasutada ning mis protseduure tuleb meetmete kasutamisel järgida.

Võrreldes Eestiga on Ühendkuningriigis julgeoleku- ja luureasutuste tegevus selgelt eraldatud politseifunktsioonidest, kuigi Ühendkuningriigis on julgeoleku- ja luureasutuste üheks ülesandeks politseijõude ja muid korrakaitseorganeid toetada nende tegevuses raskete kuritegevuse ennetamisel ja avastamisel. Erinevalt Eestist ei erista Ühendkuningriigi õigus sõjalist ja mittesõjalist julgeolekuasutuste tegevust. Suurbritannias on julgeolekuasutuste tegevuses eristatud (vastu)luure funktsioone (MI5), välisluure funktsioone (MI6) ja signaalluure funktsioone (Valitsusside Peakontor). Seega on Suurbritannias vastuluure, välisluure ja signaalluure ülesannete täitmine jaotatud selgelt julgeolekuasutuse vahel ära. Eestis teostavad aga näiteks vastuluuret ja signaalluuret nii Teabeamet kui Kaitsepolitsei. Samuti puudub Eestis eraldi asutus, mille põhiliseks ülesandeks oleks just signaalluure teostamine (Suurbritannias Valitsusside Peakontor).

Eestis on julgeolekuasutustel igal ühel teatud meetmete ring, mida ainult need asutused kasutada võivad. Suurbritannias on reguleeritud 10 erinevat meedet, mida võivad reeglina kasutada kõik julgeolekuasutused (erinevuseks on välisriikides jälitustegevuse läbiviimine, mida võivad teostada ainult MI6 ja Valitusside Peakontor). Nii Eesti kui ka Ühendkuningriigi õigus lubab osadel asutustel teostada jälitustegevust välisriikides.

Ühendkuningriigis kasutatavad meetmed on suuremas osas kasutusel ka Eestis. Kasutatavate meetmete osas seisneb olulisem erinevus Eestiga selles, et Ühendkuningriigi õigus lubab massilist andmete (näiteks inimeste terviseandmed), sh massilist sideandmete (näiteks millal, kes ja kellele helistas) kogumist suurtesse andmebaasidesse. Samuti ei ole võrreldes Ühendkuningriigiga Eestis reguleeritud krüpteeritud elektrooniliste andmete uurimist.

Eesti ja Ühendkuningriigi regulatsioonide alusel peavad julgeolekuasutused lähtuma oma tegevuses põhiõiguste kaitse ja proportsionaalsuse põhimõtetest. Samas on Ühendkuningriigi regulatsioon oluliselt detailsem, sätestades iga meetme puhul eraldi, millistel tingimustel on meetme kasutamine vajalik.

Oluline erinevus Eesti regulatsiooniga võrreldes seisneb selles, et kui Eestis on sõltuvalt meetmest vajalik kas kohtu, prokuratuuri või asutuse juhi luba või seadus loamehhanismi üldse ei reguleeri, siis Ühendkuningriigis on suurema osa meetmete jaoks vajalik ministri luba ning ülejäänud juhtudel asutuse juhi luba. Näiteks ei ole Eestis ette nähtud, et isikuandmete kogumiseks peaks saama eelnevalt loa. Suurbritannias on isikuandmete massiliseks kogumiseks vaja ministri luba.

Elektroonilise side andmete säilitamise ja kogumise osas näeb Suurbritannia regulatsioon ette, et kui sideettevõtjal sideandmed puuduvad, siis saavad luure- või julgeolekuasutused kohustada sideettevõtjat neid andmeid koguma. Eestis on sideettevõtjatel seadusest tulenev kohustus kõigi elektroonilise side andmete säilitamiseks.

Ex post järelevalve või tagatiste osas seisneb suur erinevus jälitustoimingutest teavitamise puhul. Kui Eestis on üldreegliks, et jälitustoimingutest tuleb isikut teavitada, siis Ühendkuningriigi õiguses ei ole seda ette nähtud.

Samuti seisneb oluline erinevus selles, et kui Eestis on spetsialiseerunud järelevalveasutuseks Riigikogu julgeolekuasutuste järelevalve komisjon, siis Suurbritannias teostavad järelevalvet mitmed selleks

[152] 'Extreme surveillance' becomes UK law with barely a whimper. The Guardian. 19.11.2016. https://www.theguardian.com/world/2016/nov/19/extreme-surveillance-becomes-uk-law-with-barely-a-whimper

spetsialiseerinud institutsioonid: uurimisvolituste tribunal, sideandmete jälgimise erivolinik, luureasutuste erivolinik ja Parlamendi Luure- ja Julgeolekukomisjon.

Eestist erinevalt on Ühendkuningriigis loodud eraldi uurimisvolituste tribunal, millel on jurisdiktsioon lahendada vaidlusi, mis seonduvad vaietega, mis on esitatud luure- ja julgeolekuasutuste vastu. Sellel tribunalil on ka õigus kohustada luure- või julgeolekuasutust tühistama orderit või luba, mille alusel tegevust teostatakse või kohustada luure- või julgeolekuasutust hävitama kogu informatsiooni, mis on kogutud orderi alusel või mis on luure- või julgeolekuasutusel isiku kohta.

Ühendkuningriigis on võrreldes Eestiga tugevam teenistuslik järelevalve, sest ministri kohustuseks on tagada, et meetme rakendamine oleks proportsionaalne. Lisaks on Eestist erinevalt loodud luureasutuste erivoliniku ametikoht, kelle ülesandeks on kontrolli teostamine selle üle, kas sekkuva ning suunatud jälitustegevuse, välisriikides teostatava jälitustegevuse, seadmesse sekkumise, krüpteeritud elektrooniliste andmete uurimise, varjatud inimluure allikate kasutamise ning massiliste andmete kasutamise orderid ning load on antud seaduse kohaselt ning kas neid meetmeid on teostatud seaduse kohaselt. Ühendkuningriigis on loodud ka eraldi sideandmete jälgimise erivoliniku ametikoht, kes teostab järelevalvet sideandmete hankimisel ja edastamisel sätestatud õiguste ja kohustuste täitmise üle.

Sarnaselt Eestiga on enamike järelevalveinstitutsioonide järelevalve suhteliselt „pehme“, st meetmetena saavad nad anda vaid mittesiduvaid ülevaateid, välja arvatud uurimisvolituste tribunal, millel on õigus kohustada luure- või julgeolekuasutust tühistama orderit, mille alusel tegevust teostatakse või kohustada luure- või julgeolekuasutust hävitama kogu informatsiooni, mis on kogutud orderi alusel või mis on luure- või julgeolekuasutusel isiku kohta.

Kokkuvõttes järgivad nii Eesti kui ka Ühendkuningriigi regulatsioon sarnaseid üldisemaid põhimõtteid. Julgeolekuasutuste ülesannete täitmisel on lubatud kasutada mitmesuguseid meetmeid, mis piiravad isikute põhiõiguseid, kuid meetmete rakendamisel tuleb arvestada sealjuures põhiõiguste kaitse ja proportsionaalsuse põhimõttega.

7. HOLLAND

7.1. Julgeoleku- ja luureasutused ning nende tegevust reguleerivad õigusaktid

Hollandis on kaks julgeolekuasutust:

1) **Üldine luure- ja julgeolekuteenistus** (*De Algemene Inlichtingen-en Veiligheidsdienst*, edaspidi ***AIVD***) ja
2) **Kaitseväe luure- ja julgeolekuteenistus** (*Militaire Inlichtingen-en Veiligheidsdienst*, edaspidi ***MIVD***) (WIV 2002 artikkel 6 p 1 ja artikkel 7 p 1).

Julgeoleku- ja luureasutuste tegevust reguleerib luure- ja julgeolekuseadus (*Wet op de inlichtingen- en veiligheidsdiensten 2002,* edaspidi: WIV), mis sätestab julgeolekuasutused, nende ülesanded, pädevuse ning nende kasutuses olevad meetmed.

Julgeolekuasutuste ülesannete täitmisel on oluline ka julgeolekukontrolli seadus (*Wet veiligheidsonderzoeken,* edaspidi: WVO), mis reguleerib julgeolekukontrolli läbiviimist.

Julgeolekuasutused peavad oma ülesannete täitmisel silmas pidama ka politseiseaduses (*Politiewet 2012*) sätestatut, kuna teevad koostööd politseiga, kes võib neile vajalikku informatsiooni anda. Samuti on telekommunikatsiooniseaduses (*Telecommunicatiewet*) sätestatud telekommunikatsiooni-operaatorite koostöökohustus luure- ja julgeolekuasutustega.

Julgeolekuasutuste järelevalvega seoses on olulised järgmised seadused:

1) riikliku ombudsmani seadus (*Wet Nationale ombudsman*), mis sätestab ombudsmani ülesanded ja volitused;
2) üldine haldusseadus (*Algemene wet bestuursrecht*), mis sätestab haldusorganid ja nende ülesanded;
3) esindajate koja menetlusreeglid (*Inhoudsopgave Reglement van Orde*), mis sätestab julgeolekuasutuste järelevalvekomitee ülesanded;
4) valitsuse eelarve seadus (*Comptabiliteitswet 2001*), mis sätestab auditikohtu ülesanded.

7.2. Julgeoleku- ja luureasutuste ülesanded, volitused ja meetmed põhiõiguste piiramisel

7.2.1. AIVD ja MIVD ülesanded

Üldise luure- ja julgeolekuteenistuse ehk AIVD ülesanded on sätestatud luure- ja julgeolekuseaduse artiklis 6 punktis 2 ning need on järgmised:

1) selliste inimeste ja organisatsioonide uurimine, kelle käitumine või eesmärgid annavad tõsise põhjuse kahtlustada, et nad kujutavad endast ohtu demokraatlikule õiguskorrale, riigi julgeolekule või muule Hollandi riigile olulisele hüvele (WIV 2002 art 6 p 2a);
2) julgeolekukontrolli läbiviimine viisil, mis on sätestatud julgeolekukontrolli seaduses (WIV 2002 art 6 p 2b);
3) demokraatliku õiguskorra, riigi julgeoleku ja muu Hollandi riigile olulise hüve kaitseks meetmete arendamine, sealhulgas meetmed sellise teabe kaitseks, mis peab jääma riikliku julgeoleku kaalutlustel saladuseks, ja sellise teabe kaitseks, mis kuulub avaliku teenistuse ja äriringkonna sinna ossa, mis asjaomase ministri arvamusel on olulise tähtsusega sotsiaalse korra püsimise seisukohast (WIV 2002 art 6 p 2c);
4) teiste riikide kohta käivate juurdluste läbiviimine küsimustes, mille on määranud peaminister ja üldasjade minister (*Minister van Algemene Zaken*) koostöös asjaomaste ministritega (WIV 2002 art 6 p 2d);
5) ohu- ja riskianalüüside koostamine sise- ning kuningriigi asjade ministri (*Minister van Binnenlandse Zaken en Koninkrijksrelaties*) ja julgeoleku- ning justiitsministri (*Minister van Veiligheid en Justitie*) ühisel taotlusel isikute turvalisuse tagamiseks ning objektide ja teenuste valvamiseks ja kaitsmiseks kooskõlas politseiseadusega (WIV 2002 art 6 p 2e).

Eelnevast tulenevalt teostab AIVD üksikisikute ja organisatsioonide uurimist, julgeolekukontrollide läbiviimist, elutähtsate valdkondade julgeoleku edendamist, rahvusvahelise luure teostamist ning ohu- ja riskianalüüside koostamist.

Kaitseväe luure- ja julgeolekuteenistuse ehk MIVD ülesanded on WIV artikli 7 punkti 2 alusel järgmised:

1) uurida:
   a. teiste riikide sõjalise jõu potentsiaali ja relvajõude, et selle informatsiooni alusel saavutada relvajõudude tasakaalustatud struktuur ja tõhus kasutamine (WIV 2002 art 7 punkt 2a1°);
   b. faktoreid ja sündmuseid, millega on või võivad olla seotud relvastatud jõud ning mis mõjutavad või võivad mõjutada rahvusvahelise õigussüsteemi säilitamist ja edendamist (WIV 2002 art 7 p 2a2°);
2) julgeolekukontrolli läbiviimine viisil, mis on reguleeritud julgeolekukontrolli seaduses (WIV 2002 art 7 p 2b);
3) juurdluste läbiviimine, mis on vajalikud järgnevatel eesmärkidel:
   a. nende tegevuste ärahoidmine, mille eesmärgiks on kahjustada julgeolekut või relvajõudude valmisolekut (WIV 2002 art 7 p 2c1°);
   b. mobilisatsiooni hea korralduse ja relvajõudude kontsentratsiooni edendamine (WIV 2002 art 7 p 2c2°);
   c. relvajõudude tõrgeteta ettevalmistamine ja kasutusele võtmine selliste sündmuste korral, millega on või võivad olla seotud relvastatud jõud ning mis mõjutavad või võivad mõjutada rahvusvahelise õigussüsteemi säilitamist ja edendamist (WIV 2002 art 7 p 2c3°);
4) eelmises punktis nimetatud huvide kaitseks meetmete edendamine, sealhulgas selliste meetmete, mille eesmärk on kaitsta relvajõududega seonduvat teavet vajaliku salastatuse astmega (WIV 2002 art 7 p 2d);
5) teiste riikide kohta käivate uuringute läbiviimine sõjalistes küsimustes, mille on määranud peaminister ja üldasjade minister kooskõlas asjaomaste ministritega (WIV 2002 art 7 p 2e);
6) ohuanalüüside koostamine sise- ning kuningriigi asjade ministri ja julgeoleku- ning justiitsministri ühisel taotlusel politseiseaduses nimetatud isikute turvalisuse tagamiseks ning objektide ja teenuste valvamiseks ja kaitsmiseks juhul, kui tegemist on sõjalise tähtsusega isikute, objektide ja teenustega (WIV 2002 art 7 p 2f).

Eelnevast tulenevalt teostab MIVD sõja seisukohast olulisi ülesandeid.

7.2.2. AIVD ja MIVD volitused ja meetmed

AIVD ja MIVD volitused ja meetmed on kattuvad, mistõttu käsitletakse neid järgnevalt koos. Meetmed jagunevad informatsiooni kogumise meetmeteks ning teabe töötlemiseks.

Oma ülesannete täitmisel või selleks, et neid ülesandeid korrektselt täita, on julgeolekuasutustel lubatud informatsiooni kogumiseks pöörduda järgmiste isikute poole:

1) haldusorganid, avalikud teenistujad ja isikud, kes on võimelised andma vajalikku teavet (WIV 2002 art 17 p 1a);
2) konkreetse juhtumiga seotud informatsiooni töötlemise eest vastutav isik (WIV art 17 p 1b).

Lisaks sellele on julgeolekuasutustel võimalik teabe kogumiseks kasutada järgmiseid erimeetmeid:

1) jälgimine[153] (WIV 2002 art 20 p 1a);

[153] Julgeolekuasutustel on lubatud jälgida (inglise keeles „*surveillance*“) ning selle raames salvestada informatsiooni, mis on seotud füüsiliste isikute tegevusega või informatsiooniga esemete kohta, olenemata sellest, kas jälgimiseks kasutatakse vaatlemis- või registreerimisvahendeid (WIV 2002 art 20 p 1a). Jälitustegevuse teostamisel on lubatud vaatlemis- ja registreerimisvahendite kasutamine, samuti jälgimisseadmete, asukoha

2) jälitamine[154] (WIV 2002 art 20 p 1b);
3) agentide kasutamine[155] (WIV 2002 art 21);
4) juriidiliste isikute loomine[156] (WIV 2002 art 21 p 1b);
5) läbiotsimine[157] (WIV 2002 art 22 p 1a, 1b ja 1c);
6) saadetiste avamine[158] (WIV 2002 art 23 p 1);
7) elektroonilisse seadmesse sisenemine[159] (WIV 2002 art 24 p 1a, 1b a 1c);
8) pealtkuulamine[160] (WIV 2002 art 25 p 1);
9) välisriigi side salvestamine[161] (WIV 2002 art 26 p 1);
10) mittespetsiifilise side salvestamine[162] (WIV 2002 art 27 p 1);
11) sideoperaatorite poole pöördumine[163] (WIV art 28 p 1, WIV 2002 art 29 p 1).

Sealjuures täpsustab WIV 2002 artikkel 18, milliste konkreetse ülesannete täitmisel on AIVD-l ja MIVD-l eelnevalt nimetatud erimeetmeid kasutada. Näiteks on lubatud AIVD-l neid meetmeid kasutada eelmises alapeatükis (7.2.1) punktis 1 ja 4 loetletud ülesannete täitmiseks. MIVD-l on lubatud aga kasutada neid meetmeid eelmises alapeatükis (7.2.1) punktis 1, 3a, 3c ja 5 loetletud ülesannete täitmiseks.

Julgeolekukontrolli läbiviimiseks ei ole eelnevalt nimetatud erimeetmeid lubatud kasutada. Julgeolekukontrolli läbiviimisel teevad asutused isikule taustauuringu, mis sisaldab riikliku julgeoleku

positsioneerimise seadmete ja salvestamisvahendite paigaldamine. Neid seadmeid võib siiski kasutada ruumides, mis ei ole Kaitseministeeriumi kasutuses (WIV 2002 art 20 p 2).

[154] Julgeolekuasutustel on lubatud jälitada (inglise keeles: „*trace*“) ja selle raames salvestada informatsiooni, mis on seotud füüsiliste isikutega või informatsiooniga esemete kohta, olenemata sellest, kas jälgimiseks ja salvestamiseks kasutatakse jälgimisseadmeid (inglise keeles: „*tracing instruments*“), asukoha positsioneerimise seadmeid (inglise keeles: „*location positioning equipment*“) ja salvestamisvahendeid (inglise keeles: „*registration instruments*“) (WIV 2002 art 20 p 1b). Jälitada võib siiski ainult sellistes ruumides, mis ei ole Kaitseministeeriumi kasutuses (WIV 2002 art 20 p 2).

[155] Julgeolekuasutustel on lubatud kasutada agentidena füüsilisi isikud, olenemata sellest, kas nad esinevad mingi muu isikuna või mitte, ning juhendada neid asutuse vastutusel koguma otseselt informatsiooni (inglise keeles: „collecting in a directed way“) või võtma kasutusele meetmed, et kaitsta asutuse huve (WIV 2002 art 21 p 1a). Asjakohane minister saab kohustada haldusorganeid tegema koostööd nii, et nad varustavad agendina kasutatava füüsilise isiku uue identiteediga (inglise keeles: „assumed identity“) ((WIV 2002 art 21 p 2).

[156] Julgeolekuasutustel on lubatud luua ja kasutada juriidilisi isikuid julgeolekuasutuse tegevuse toetuseks (inglise keeles: „in support of operational activities“) (WIV 2002 art 21 p 1b).

[157] Julgeolekuasutustel on lubatud tehnilise vahendiga või ilma otsida läbi kinniseid ruume, otsida läbi suletud objekte, viia läbi uurimist objektidel eesmärgiga tuvastada isiku identiteet.

[158] Julgeolekuasutustel on lubatud avada kirju ja muid adresseeritud saadetisi ilma saatja või adressaadi loata.

[159] Julgeolekuasutustel on lubatud elektroonilisse seadmesse sisenemine tehnilise vahendi, valesignaali, valevõtmete, valeidentiteedi abil või ilma nendeta. Elektroonilisse seadusmesse sisenemise õigus hõlmab ka õigust turvameetmetest läbi murda, õigust kasutada tehnilisi abivahendeid krüpteeritud informatsiooni kättesaamiseks ning õigust kopeerida salvestatud andmeid.

[160] Luure- või julgeolekuasutusel on lubatud tehnilise seadme abiga pealt kuulata, vastu võtta, salvestada ja otseselt jälgida mistahes vormis vestlust, telekommunikatsiooni või automatiseeritud andmeedastust, sõltumata sellest, kus see aset leiab. Volitus hõlmab ka vestluse, telekommunikatsiooni või automatiseeritud andmeedastuse krüpteerimisest vabastamist.

[161] Luure- või julgeolekuasutusel on lubatud tehnilise seadme abiga vastu võtta ja salvestada raadiosidet, mis pärineb selle tehnilise iseloomu põhjal otsustades teistest riikidest või on mõeldud teistesse riikidesse edastamiseks.

[162] Luure- või julgeolekuasutusel on lubatud tehnilise seadme abiga vastu võtta ja salvestada mittespetsiifilist raadiosidet. Selleks mittespetsiifiliseks sideks on näiteks satelliidiside. Järelevalvekomitee (the Review Committee on the Intelligence and Security Services) aruanne, lk 5. Kättesaadav Internetis: https://english.ctivd.nl/investigations/r/review-report-24/documents

[163] Luure- või julgeolekuasutusel on lubatud pöörduda üldkasutatavate sidevõrkude ja sideteenuste pakkujate poole sooviga saada teavet kasutaja ja temaga seonduva side kohta. Lisaks on Luure- või julgeolekuasutusel lubatud pöörduda üldkasutatavate sidevõrkude ja sideteenuste pakkujate poole sooviga saada informatsiooni seoses isiku nimega, aadressiga, postiindeksiga, elukohaga või teenuse tüübiga, mis kasutajal on.

seisukohast olulise informatsiooni uurimist (WVO artikkel 7 p 2). Julgeolekukontroll algab asutuse enda andmebaasidest informatsiooni kogumisega. Informatsioon, millele enim keskendutakse, hõlmab isiku karistusregistri väljavõtteid, demokraatiavastaseid tegevusi, sõltuvusi, varalist kindlustatust, ebasobivaid mõjutusi isikule, ebaausat või saladuslikku käitumist, aususe puudumist ning riskikäitumist. Olenevalt töökohast on teatud juhtudel vajalik ka intervjuu läbiviimine nii isiku enda kui ka tema lähedastega.[164]

Julgeolekuasutustel on lubatud töödelda teavet, järgides luure- ja julgeolekuseaduses või julgeolekukontrolli seaduses kehtestatud nõudeid (WIV 2002 art 12 p 1).

Asutuste ametnikel ei ole õigust uurida süütegusid (WIV 2002 art 9 p 1). Seega ei ole AIVD-il ega MIVD-il õiguskaitse funktsioone ja neil ei ole lubatud kedagi arestida või kinni pidada (WIV 2002 art 9 p 2).

Nii AIVD kui ka MIVD võivad tegutseda välismaal tulenevalt oma ülesannetest, mis on sätestatud WIV 2002 artiklites 6 ja 7.[165]

7.3. Protseduurid põhiõiguste riive õiguspärasuse tagamiseks

Luure- ja julgeolekuseaduse alusel peavad julgeolekuasutused oma tegevusel lähtuma seaduses sätestatud põhimõtetest, mida käsitletakse järgnevalt.

Informatsiooni kogumiseks erivolituste kasutamisel on vajalik järgida järgnevaid üldiseid põhimõtteid:

1) informatsiooni kogumiseks kasutatavaid meetmeid võib kasutada ainult siis, kui see on vajalik ülesande täitmiseks (vajalikkuse põhimõte) (WIV 2002 art 18 ja art 12);
2) kasutatavatest meetmetest tuleb valida isikut kõige vähem koormav meede arvestades meetmega kaitstava huve ähvardavat ohu tõsidust (proportsionaalsuse põhimõte) (WIV 2002 art 31);
3) meetme kasutamine tuleb koheselt lõpetada, kui meetme kasutamise eesmärk on täidetud või kui vähemkoormava meetme kasutamine on võimalik (subsidiaarsuse põhimõte) (WIV 2002 art 32);
4) üldjuhul võib meetmeid kasutusele võtta ainult siis, kui asjaomane minister (AIVD-i ülesannetega seoses sise- ja kuningriigi asjade minister ning MIVD-i ülesannetega seoses kaitseminister (WIV 2002 art 1 p c1o ja p c2o)) või asjaomane asutuse juhataja annab selleks loa (WIV 2002 art 19 p 1). Üldjuhul saab loa meetmete kasutamiseks kolmeks kuuks, seda perioodi on võimalik pikendada eraldi taotluse alusel (WIV 2002 art 19 p 3).

Julgeolekuasutustel on teatud juhtudel ka isikute teavitamiskohustus (WIV 2002 art 34 p 1). Asjakohane minister uurib pärast viie aasta möödumist erinevate erivolituse kasutamisest (saadetiste avamine, pealtkuulamine, mittespetsiifilise kommunikatsiooni salvestamine (mis on salvestatud näiteks isikust tingitult), juurdepääsu saamine eluruumidele ilma elaniku loata) ning seejärel kord aastas, kas isikule, kelle suhtes erivolitust kasutati, saab meetmete kasutamise kohta aruande esitada. Kui see on võimalik, toimub teavitamine nii kiiresti kui võimalik.

Lisaks üldistele põhimõtetele kohaldub järgnevatele meetmetele eriregulatsioon.

(a) Informatsiooni kogumine

Jälgimist (kasutades jälgimis- ja registreerimisvahendeid) võib teostada ainult siis, kui selleks on andnud loa sise- ja kuningriigi asjade minister või AIVD-i juht (juhul kui minister on selle AIVD juhile delegeerinud) (WIV 2002 art 20 p 2 ja 3, art 19 p 1). Kui jälgimist teostatakse eluruumides, võib loa anda ainult asjaomane minister. Loa saamise taotluses peab olema märgitud selle koha aadress, kus

[164] General Intelligence and Security Service. Positions involving confidentiality and security screening, lk 3-4.
[165] Supervisory Committee on the Intelligence and Security Services CTIVD no. 8a and no. 8b Supervisory Report

jälitustegevust teostatakse, kasutatava elektroonilise instrumendi kirjeldus ning põhjus, miks selle instrumendi kasutamine on vajalik (WIV 2002 art 20 p 4).

Jälitamine. Jälitamis- ja asukoha positsioneerimisvahendite kasutamine on lubatud ainult siis, kui selleks on andnud loa sise- ja kuningriigi asjade minister või AIVD-i juht (juhul kui minister on selle AIVD juhile delegeerinud) (WIV 2002 art 20 p 2 ja 3). Eluruumides on jälitamine lubatud ainult siis, kui loa on andnud sise- ja kuningriigi asjade minister (WIV 2002 art 20 p 3). Loa saamise taotluses peab olema märgitud aadress, kus kavatsetakse seadet kasutada, kasutatava seadme kirjeldus ning põhjendus, miks vastava seadme kasutamine on vajalik (WIV 2002 art 20 p 4).

Läbiotsimine. Kinniste ruumide ja objektide läbiotsimine ning uurimise läbiviimine objektidel, mille eesmärgiks on isiku identiteedi tuvastamine, on lubatud ainult ministri või AIVD-i juhi loal (WIV art 22 p 2). Kinniste eluruumide läbiotsimist võib teostada vaid siis, kui asjaomane minister on selleks asutuse juhatajale oma kirjaliku nõusoleku andnud. Kui läbiotsimist teostab MIVD, siis on luba vaja sise- ja kuningriigi asjade ministrilt (WIV 2002 art 22 p 4). Luba antakse maksimaalselt kolmeks päevaks (WIV 2002 art 22 p 5). Asutuse juhataja peab muuhulgas loa taotlemisel tooma välja põhjuse, miks läbiotsimine vajalik on (WIV 2002 art 22 p 6b).

Saadetiste avamine. Õigus avada kirju ja muid adresseeritud saadetisi ilma saatja või adressaadi loata on juhul, kui Haagi kohus on selleks selle asutuse juhataja taotlusel andnud välja korralduse (WIV 2002 art 23 p 1). Korraldus antakse maksimaalselt kolmeks kuuks (WIV 2002 art 23 p 6b). Asjaomase ministri nõusolek vajalik ei ole (WIV 2002 art 23 p 2). Korralduse taotlemisel peab muuhulgas välja tooma põhjuse, miks vastavat saadetist on vaja avada (WIV 2002 art 23 p 4b).

Elektroonilisse seadmesse sisenemine. Elektroonilisse seadmesse sisenemiseks peab loa andma sise- ja kuningriigi asjade minister või AIVD juht (juhul kui minister on selle AIVD juhile delegeerinud) (WIV 2002 art 24 p 2).

Pealtkuulamine. Elektroonilise seadme abil mistahes vormis vestluse, side või automatiseeritud andmeedastuse pealtkuulamiseks, vastuvõtmiseks, salvestamiseks või otseseks jälgimiseks peab loa andma julgeoleku- või luureasutuse juht (WIV 2002 art 25 p 2). Kui eelnimetatud tegevusi teostab MIVD, siis on luba vaja sise- ja kuningriigi asjade ministrilt (WIV 2002 art 25 p 3). See ei kehti raadioside vastuvõtu ja registreerimise puhul, mis on pärit teistest riikidest või mõeldud teistesse riikidesse edastamiseks. Kui side on seotud sõjalise sõnumiga, siis ei ole vajalik ministri luba (WIV 2002 art 25 p 8). Loa taotlemisel peab taotlus sisaldama: (i) selle meetme kirjeldust, mida asutust soovib kasutada; (ii) isiku või organisatsiooni andmeid, kellega seoses meetmeid soovitakse kasutada; (iii) põhjendus, miks soovitakse meedet kasutada. (WIV 2002 art 25 p 4c).

Välisriigi side salvestamine. Selleks, et vastu võtta ja salvestada raadiosidet, mis on pärit teistest riikidest või mõeldud teistesse riikidesse saatmiseks, ei ole asjaomase ministri nõusolek vajalik (WIV 2002 art 26 p 2). Kui vastava informatsiooni kogumine ei ole vajalik asutuse ülesande täitmiseks, siis saadud informatsioon hävitatakse viivitamatult (WIV 2002 art 26 p 5).

Mittespetsiifilise side salvestamine. Asjaomase ministri nõusolek ei ole vajalik, et mittespetsiifilist raadiosidet vastu võtta ja salvestada (WIV 2002 art 27 p 2). Saadud informatsiooni võib üldjuhul talletada 1 aasta (WIV 2002 art 27 p 9).

Kuigi mittespetsiifilise raadioside vastuvõtmiseks ja salvestamiseks ei ole ministri luba vaja, siis selle kommunikatsiooni sisu teada saamiseks on luba vajalik. Kui side, mille sisu soovitakse teada saada, valiti selle põhjal, et see sisaldab informatsiooni isiku või asutuse kohta, siis on vajalik sise- ja kuningriigi asjade ministri luba. See luba antakse maksimaalselt kolmeks kuuks, kuid seda on võimalik pikendada. Loa taotlemisel tuleb muuhulgas tuua välja, miks vastav valik tehakse (WIV 2002 art 27 p 4). Kui kommunikatsiooni sisu soovitakse teada saada selle põhjal, et see sisaldab teatud fraasi (*catchphrase*), siis tuleb luba saada asjaomaselt ministrilt ning see antakse üheks aastaks, mida samuti saab pikendada (WIV 2002 art 27 p 5).

Sideoperaatorite poole pöördumine. Asjaomase ministri nõusolek ei ole vajalik siis, kui pöördutakse sidevõrkude ja sideteenuste pakkujate poole, et saada informatsiooni side toimumise kohta (WIV 2002 art 28 p 2). Informatsioon sisaldab andmeid selle kohta, mis numbrilt kellele kõne tehti, kellele see number kuulub ning kõne aeg ja kestvus. Kuigi pöördumiseks ei lähe ministri luba vaja, saab sellise

pöördumise teha ainult AIVD-i või MIVD-i juht, kes on selle kooskõlastanud AIVD-i juhiga (WIV 2002 art 28 p 4).

(b) Teabe töötlemine

Informatsiooni töötlemine toimub ainult kooskõlas WIV-i regulatsiooniga ning üksnes sellel eesmärgil, et luure- ja julgeolekuasutused saaksid täita oma ülesandeid (vt üleval p 1.2). (WIV 2002 art 12 p-d 1 ja 2). Töödelda võib ainult sellist informatsiooni, mis on seotud järgmiste isikutega:

1) isik, kes annab põhjuse arvata, et ta on tõsiseks ohuks demokraatlikule korrale või relvajõudude turvalisusele ja valmisolekule;
2) isik, kes on andnud loa julgeolekukontrolli läbiviimiseks;
3) isik, kelle osas see on vajalik seoses uurimistega, mis on seotud teiste riikidega;
4) isik, kelle kohta on informatsiooni kogunud teised luure- ja julgeolekuasutused;
5) isik, kelle andmed on vajalikud, et asutus saaks oma ülesandeid täita (WIV 2002 art 12 p 1 ja p 2). Seadus ei täpsusta, milliseid ülesandeid see hõlmab, aga eelduslikult mõeldakse siin ülesandeid, mis on WID-s sätestatud (vt üleval p 1.2);
6) isik, kes töötab või on töötanud MIVD-is või AIVD-is.

Isikuandmed ei või töödelda isiku usutunnistuse, veendumuste, rassi, tervise või seksuaalelu kohta (WIV 2002 art 13 p 3).

7.4. Järelevalve korraldus julgeoleku- ja luureasutuste tegevuse õigus- ja eesmärgipärasuse üle

(a) Täitevvõim

Täitevvõimu ülesandeks on julgeolekuasutuste üldise poliitika ja prioriteetide määratlemine. Sealhulgas võib täitevvõim kehtestada julgeolekuasutustele reegleid. Täitevvõim on ka poliitiliselt vastutav julgeolekuasutuste eest ja peab parlamendile nende tegevusest aru andma. Samuti peab vastavalt kas sise- ja kuningriigi asjade minister või kaitseminister volitama julgeolekuasutusi, et nad saaksid kasutada neile antud erivolitusi.

Kord aastas annavad asjaomased ministrid aru kahele Generaalstaatide Kojale (hollandi keeles: „*kamers der Staten-Generaal*“; inglise keeles: „*Chambers of the States General*“), kuidas AIVD ning MIVD on oma ülesandeid täitnud (WIV 2002 art 8 p 1). Asjaomased ministrid on: AIVD-i ülesannetega seoses sise- ja kuningriigi asjade minister ning MIVD-i ülesannetega seoses kaitseminister (WIV 2002 art 1 p c1º ja p c2º). Asjaomane minister võib kehtestada täpsemad reeglid asutuse kui organisatsiooni töömeetodite ja korralduse kohta (WIV 2002 art 11).

(b) Parlament

Hollandi parlamendi Esindajate Kojal (hollandi keeles: „*Tweede Kamer*“; inglise keeles: „*The House of Representatives*“) on julgeoleku ja turvalisuse komitee. Komitee koosneb erakondade juhtidest Hollandi parlamendi madalamas kojas. Komiteel on õigus jälgida mistahes luureteenistuse töö aspekte ja neil on juurdepääsuõigus kogu asjakohasele teabele. Reeglid selleks on sätestatud Esindajate Koja käitumisreeglites (esindajate koja käitumisreeglid art 10 p 1; art 22 p 1). Praktikas ei teosta komitee igapäevast järelevalvet julgeolekuasutuste üle ega vii läbi juurdlusi, sest neid ülesandeid täidab järelevalvekomitee (inglise keeles: „*the Review Committee on the Intelligence and Security Services*“).[166]

Järelevalvekomitee on vastutav luure- ja julgeolekuseaduse ning julgeolekukontrolli seaduse sätete täitmise seaduslikkuse järelevalve üle. Lisaks on järelevalvekomitee ülesandeks asjaomaste ministrite teavitamine ja nõustamine seoses komitee leidudega ning seoses juurdluste ja kaebuste hindamisega

[166] Intelligence Legislation Model: The Netherlands Intelligence and Security Services Act, 2002, lk 8.

(WIV 2002 art 64 p 2). Komitee koosneb kolmest liikmest (WIV 2002 art 65 p 1). Liikmed nimetab ametisse Kuninglik Dekreet (hollandi keeles: „*koninklijk besluit*“, inglise keeles: „*Royal Decree*“) asjakohase ministri ettepanekul kuueks aastaks.

Järelevalvekomiteel on taotluse alusel vahetu juurdepääs asjakohasele informatsioonile (WIV 2002 art 73 p 1). Järelevalvekomitee võib paluda isikutel ilmuda enda ette informatsiooni edastamiseks tunnistajana või eksperdina (WIV 2002 art 74 p 1). Järelevalvekomitee taotlus tuleb esitada kirjalikult ning peab andma võimalikult täpse ülevaate, mille kohta tunnistaja või ekspert komiteele informatsiooni andma peab (WIV 2002 art 74 p 2). Isikutel ei ole õigust keelduda informatsiooni andmisest, kuid neid võib esindada advokaat, kui nad peavad isiklikult järelevalvekomitee ette minema (WIV 2002 art 74 p 3).

Järelevalvekomitee võib läbi viia juurdlusi, et kontrollida, kas luure- ja julgeolekuasutused on järginud WIV-i regulatsiooni (WIV 2002 art 78 p 1). Pärast juurdluse läbiviimist koostab järelevalvekomitee raporti, mis on avalik. Enne raporti avalikustamist annab komitee asjakohasele ministrile võimaluse raportiga tutvuda ning esitada selle kohta omapoolseid seisukohti. Järelevalvekomiteel on õigus teha juurdluse tulemuste põhjal asjakohasele ministrile ettepanekuid meetmete osas, mida tuleks kasutusele võtta.

(c) Ombudsman

Riiklik ombudsman võib vastu võtta ja uurida kaebusi seoses julgeolekuasutuste tegevusega (WIV 2002 art 83 p 1). Samas tuleb isikutel enne ombudsmani poole pöördumist esitada kaebus asjaomasele ministrile. Asjaomane minister (AIVD-i ülesannetega seoses sise- ja kuningriigi asjade minister ning MIVD-i ülesannetega seoses kaitseminister (WIV 2002 art 1 p c1o ja p c2o) peab kaebuse saamisel nõu järelevalvekomiteega (WIV 2002 art 83 p-d 2 ja 3). Kui isik ei jää rahule sellega, kuidas tema kaebust käsitleti, on tal õigus pöörduda ombudsmani poole (WIV 2002 art 83 p 2). Ombudsman võib teha ministrile ettepanekuid, milliseid meetmeid tuleks kaebuse käsitlemisel kasutusele võtta (WIV 2002 art 84 p 2).

7.5. Julgeoleku- ja luureasutuste volitused ja meetmed elektroonilise side jälgimisel ning andmete töötlemisel ja talletamisel

(a) Informatsiooni kogumine

Elektroonilisse seadmesse sisenemine võib toimuda tehnilise vahendi, valesignaali, valevõtmete, valeidentiteedi abil või ilma nendeta. Elektroonilisse seadmesse sisenemise õigus hõlmab ka õigust turvameetmetest läbi murda, õigust kasutada tehnilisi abivahendeid krüpteeritud informatsiooni kättesaamiseks ning õigust kopeerida salvestatud andmeid (WIV 2002 art 24 p 1a, 1b a 1c). Elektroonilisse seadmesse sisenemiseks peab loa andma sise- ja kuningriigi asjade minister või teatud juhtudel AIVD juht (WIV 2002 art 24 p 2).

Pealtkuulamine. Asutustel on lubatud tehnilise seadme abiga kuulata, vastu võtta, salvestada ja otseselt jälgida mis tahes vormis vestlust, side ja andmeside elektroonilise seadme abil, sõltumata sellest, kus see aset leiab. Volitus hõlmab ka dekrüpteerimist (WIV 2002 art 25 p 1). Elektroonilise seadme abil mistahes vormis vestluse, side või automatiseeritud andmeedastuse pealtkuulamiseks, vastuvõtmiseks, salvestamiseks või otseseks jälgimiseks peab loa andma julgeoleku- või luureasutuse juht (WIV 2002 art 25 p 2). Kui eelnimetatud tegevusi teostab Kaitseväe luure- ja julgeolekuteenistus, siis on vaja sise- ja kuningriigi asjade ministrilt luba (WIV 2002 art 25 p 3). See ei kehti sellise raadioside vastuvõtu ja registreerimise puhul, mis on pärit teistest riikidest või mõeldud teistesse riikidesse edastamiseks. Kui side on seotud sõjalise sõnumiga, siis ministri luba vajalik ei ole (WIV 2002 art 25 p 8). Loa taotlus peab sisaldama: (i) selle meetme kirjeldust, mida asutust soovib kasutada; (ii) isiku või organisatsiooni andmeid, kellega seoses meetmeid soovitakse kasutada; (iii) põhjendus, miks soovitakse meedet kasutada (WIV 2002 art 25 p 4c).

Välisriigi side salvestamine. Selleks, et vastu võtta ja salvestada raadiosidet, mis on pärit teistest riikidest või mõeldud teistesse riikidesse saatmiseks, ei ole asjaomase ministri nõusolek vajalik (WIV

2002 art 26 p 2). Kui vastava informatsiooni kogumine ei ole vajalik asutuse ülesande täitmiseks, siis saadud informatsioon hävitatakse viivitamatult (WIV 2002 art 26 p 5).

Mittespetsiifilise side salvestamine. Asutustel on lubatud tehnilise seadme abiga vastu võtta ja salvestada mittespetsiifilist raadiosidet (WIV 2002 art 27 p 1). Asjaomase ministri nõusolek ei ole vajalik, et mittespetsiifilist raadiosidet vastu võtta ja salvestada (WIV 2002 art 27 p 2). Saadud informatsiooni võib üldjuhul talletada 1 aasta (WIV 2002 art 27 p 9).

Kuigi mittespetsiifilise raadioside vastuvõtmiseks ja salvestamiseks ei ole ministri luba vaja, siis selle kommunikatsiooni sisu teada saamiseks on luba vajalik. Kui side, mille sisu soovitakse teada saada, valiti selle põhjal, et see sisaldab informatsiooni isiku või asutuse kohta, siis on vajalik sise- ja kuningriigi asjade ministri luba. See luba antakse maksimaalselt kolmeks kuuks ning seda on võimalik pikendada. Loa taotlemisel tuleb muuhulgas tuua välja, miks vastav valik tehakse (WIV 2002 art 27 p 4). Kui kommunikatsiooni sisu soovitakse teada saada selle põhjal, et see sisaldab teatud fraasi (*catchphrase*), siis tuleb luba saada asjaomaselt ministrilt ning see antakse üheks aastaks ning seda on võimalik pikendada (WIV 2002 art 27 p 5).

Sideoperaatorite poole pöördumine. Asjaomase ministri nõusolek ei ole vajalik siis, kui pöördutakse sidevõrkude ja sideteenuste pakkujate poole, et saada informatsiooni side toimumise kohta (WIV 2002 art 28 p 2). See informatsioon sisaldab informatsiooni selle kohta, mis numbrilt ning kellele kõne tehti, kellele see number kuulub ning kõne aeg ja kestvus. Kuigi pöördumiseks ei lähe ministri luba vaja, saab sellise pöördumise teha ainult AIVD-i juhataja või siis MIVD-i juhataja, kui ta on selle kooskõlastanud AIVD-i juhatajaga (WIV 2002 art 28 p 4).

(b) Teabe töötlemine

Julgeolekuasutustel on lubatud töödelda teavet, järgides luure- ja julgeolekuseaduses või julgeolekukontrolli seaduses kehtestatud nõudeid (WIV 2002 art 12 p 1).

Informatsiooni töötlemine toimub ainult kindlal eesmärgil (WIV 2002 art 12 p 2) ja ainult sellises ulatuses, mis on vajalik WIV-i rakendamiseks. Kindla eesmärgiga on tegu siis, kui isikuandmete töötlemine on seotud järgmiste isikutega:

1) isik, kes annab põhjuse arvata, et ta on tõsiseks ohuks demokraatlikule korrale või relvajõudude turvalisusele ja valmisolekule;
2) isik, kes on andnud loa julgeolekukontrolli läbiviimiseks;
3) isik, kelle osas see on vajalik seoses uurimistega, mis on seotud teiste riikidega;
4) isik, kelle kohta on informatsiooni kogunud teised luure- ja julgeolekuasutused;
5) isik, kelle andmed on vajalikud, et asutus saaks oma ülesandeid täita (WIV 2002 art 12 p 1 ja p 2). Seadus ei täpsusta, milliseid ülesandeid see hõlmab, aga eelduslikult mõeldakse siin ülesandeid, mis on WID-s sätestatud (vt üleval p 1.2);
6) isik, kes töötab või on töötanud MIVD-is või AIVD-is.

Isikuandmed ei või töödelda isiku usutunnistuse, veendumuste, rassi, tervise või seksuaalelu põhjal (WIV 2002 art 13 p 3).

7.6. Järeldused läbivate üldpõhimõtete kohta julgeoleku- ja luureasutuste tegevuse reguleerimisel ning elluviimisel

Hollandis on julgeolekuasutustega seonduv regulatsioon süstematiseeritud ning koondunud luure- ja julgeolekuseadusesse, mida täiendab julgeolekukontrolli seadus. Luure- ja julgeolekuseaduse järgi teostab MIVD üksikisikute ja organisatsioonide uurimist, julgeolekukontrollide läbiviimist, elutähtsate valdkondade julgeoleku edendamist, rahvusvahelise luure teostamist ning ohu- ja riskianalüüside koostamist ning AIVD teostab sarnaseid ülesandeid lähtuvalt sõjalisest seisukohast. Asutuste ametnikel ei ole õigust uurida süütegusid ja neil ei ole lubatud kedagi arestida või kinni pidada, seega on julgeolekuasutused selgelt eristatud politseist.

Julgeolekuasutustele on antud laiaulatuslikud volitused oma ülesannete teostamisel, kuid seejuures on tähelepanu pööratud ka põhiõiguste kaitsele. Luure- ja julgeolekuseadus, mis reguleerib kahe julgeolekuasutuse ülesandeid, pädevust ning nende kasutuses olevaid meetmeid, võttis Parlament vastu 2002. aastal pärast seda kui Riiginõukogu (kõrgeim halduskohus) leidis, et teatud kehtiva seaduse osad ei ole kooskõlas Euroopa inimõiguste konventsiooniga ja Euroopa Inimõiguste Kohtu praktikaga.[167] Seega, võttes arvesse kehtivas regulatsioonis sätestatud meetmete kasutamise protseduure ja järelevalvesüsteemi, on põhiõiguste kaitse julgeolekuasutuste regulatsioonis olulisel kohal.

7.7. Hollandi ja Eesti regulatsioonide võrdlus

Julgeolekuasutustega seonduv regulatsioon on Eestis killustatud ning sisaldub paljudes õigusaktides. Erinevalt Eestist on Hollandi julgeolekuasutustega seonduv regulatsioon süstematiseeritud ning koondunud luure- ja julgeolekuseadusesse, mida täiendab julgeolekukontrolli seadus.

Erinevalt Eestist täidavad Hollandis riigile vajalikke luurefunktsioone mõlemad julgeolekuasutused ning luure erinevad funktsioonid pole jagatud mitme asutuse vahel nagu Eestis. Nii Hollandis kui ka Eestis ei ole sõjaliste ja mittesõjaliste julgeolekuasutuste ülesanded selgelt eristatavad ning on mitmeti kattuvad.

Eesti julgeolekuasutustel on igal ühel teatud meetmete ring, mida ainult nemad kasutada võivad. Hollandis on reguleeritud 11 erinevat meedet, mida võivad kasutada mõlemad julgeolekuasutused, seega on mõlema Hollandi julgeolekuasutuse meetmed ja volitused kattuvad.

Julgeolekuasutuste ülesanded, volitused ja meetmed on üldises plaanis Eestis ja Hollandis sarnased, olulise erinevusena saab välja tuua korrakaitselise tegevuse ja kriminaaluurimise. Erinevalt Eestist on Hollandis julgeoleku- ja luureasutuste tegevus selgelt eraldatud politseifunktsioonidest, julgeolekuasutustel ei ole lubatud uurida süütegusid ega tegeleda korrakaitseliste ülesannetega. Sellest tulenevalt ei ole Hollandis sätestatud meetmena isiku kaasamist salajasele koostööle, konspiratsioonivõtete kasutamist, teesklemist või variisiku kasutamist nagu seda on Eestis Kaitsepolitseil vastuluures kasutatavate meetmetena. Kuivõrd Hollandi julgeolekuasutused ei uuri süütegusid, puuduvad Hollandi julgeolekuasutustel süütegude menetlemiseks kasutatavad meetmed nagu seda on Eestis. Samuti puuduvad teatud korrakaitseks kasutatavad meetmed nagu sundtoomise kohaldamine ning isiku kinnipidamine (Hollandi julgeolekuasutustel ei ole õigust kedagi arestida või kinni pidada).

Võrreldes Hollandiga ei ole Eestis reguleeritud krüpteeritud elektrooniliste andmete uurimist. Hollandis hõlmab igasugune elektroonilisse seadmesse sisenemine ka õigust turvameetmetest läbi murda, õigust kasutada tehnilisi abivahendeid krüpteeritud informatsiooni kättesaamiseks ning õigust kopeerida salvestatud andmeid.

Mõlemas riigid peavad julgeolekuasutused oma tegevusel lähtuma seaduses sätestatud põhimõtetest. Nii Eestis kui ka Hollandis võib meetmeid kasutada vaid siis, kui see on proportsionaalne. Kohustus teavitada isikut, kelle sõnumi saladust ja kodu, perekonna- või eraelu puutumatuse õigust on piiratud, on nii Eestis kui ka Hollandis. Oluline erinevus Eesti regulatsiooniga võrreldes seisneb selles, et kui Eestis on sõltuvalt meetmest vajalik kas kohtu luba, prokuratuuri luba, asutuse juhi luba või seadus loamehhanismi üldse ei reguleeri, siis Hollandis on suurema osa meetmete jaoks vajalik ministri luba ning ülejäänud juhtudel asutuse juhi luba (vaid ühel juhul on vajalik kohtu luba).

Järelevalve on üldjoontes mõlemas riigis sarnane. Julgeolekuasutuste üle teostavad järelevalvet vastavad ministrid, kes peavad omakorda parlamendile ülevaate koostama. Hollandis peavad ministrid aru andma kord aastas, Eestis vähemalt korra kuue kuu jooksul.

Mõlemas riigis teostab põhilist järelevalvet vastav parlamendi komisjon: Hollandis järelevalvekomitee, Eestis Riigikogu julgeolekuasutuste järelevalve komisjon. Kui Eestis on julgeolekuasutuste järelevalve komisjon Riigikogu erikomisjon, siis Hollandis koosneb komitee kolmest liikmest, kes nimetatakse ametisse kuueks aastaks. Hollandi parlamendi Esindajate Kojal on ka julgeoleku ja turvalisuse komitee,

[167] Intelligence Legislation Model: The Netherlands Intelligence and Security Services Act, 2002, lk 8.

kuid praktikas ei teosta komitee igapäevast järelevalvet julgeolekuasutuste üle ega vii läbi juurdlusi, sest neid ülesandeid täidab järelevalvekomitee.

Nii Eestis kui ka Hollandis teostab järelevalvet ka ombudsman (Eestis õiguskantsler). Erinevalt Eestist on Hollandis ombudsman järelevalvega seotud läbi kaebuste seoses julgeolekuasutuste tegevusega. Eestis on õiguskantsleri pädevuses kontrollida julgeoleku- ja luureasutuste tegevust nii luure/vastuluure, korrakaitse kui ka kriminaalmenetluse raames ning järelevalve võib toimuda ka omaalgatuslikult. Erinevalt Eestist ei teosta järelevalveasutuste üle Hollandis järelevalvet prokuratuur, samuti puudub Hollandis jälitustoimingute infosüsteem.

Kokkuvõttes järgivad nii Eesti kui ka Hollandi regulatsioon sarnaseid üldisemaid põhimõtteid. Julgeolekuasutuste ülesannete täitmisel on lubatud kasutada mitmesuguseid meetmeid, mis piiravad isikute põhiõiguseid, kuid meetmete rakendamisel tuleb arvestada sealjuures põhiõiguste kaitse põhimõttega.

8. SAKSAMAA

8.1. Julgeoleku- ja luureasutused ning nende tegevust reguleerivad õigusaktid

Saksamaal on kolm julgeolekuasutust:

1) **Riiklik Konstitutsioonikaitse Amet** (Bundesamt für Verfassungsschutz – **BfV**);
2) **Militaarne Vastuluure** (Der Militärischen Abschirmdienst - **MAD**); ning
3) **Riiklik Luureteenistus** (Bundesnachrichtendienst – **BND**).

Riiklik Konstitutsioonikaitse amet (BfV) allub Siseministeeriumile, Militaarse Vastuluure amet (MAD) Kaitseministeeriumile ning Riiklik Luureteenistus (BND) Riigikantseleile.

Riikliku Konstitutsioonikaitse Ameti alluvuses on **Liidumaa Konstitutsioonikaitse Ametid** (Landesämter für Verfassungsschutz – **LfV**).

Saksamaal on iga julgeolekuasutuse tegevus reguleeritud eraldi seadusega.

Riikliku Konstitutsioonikaitse Ameti seadus (Verbindung mit dem Bundesverfassungsschutzgesetz, edaspidi: *BVerfSchG*) sätestab Riikliku Konstitutsioonikaitse Ameti ning ka Liidumaa Konstitutsioonikaitse ametite volitused, meetmed ja muu tegevuse. **BVerfSchG reguleerib julgeolekuasutuste üldosaseadusena ka teiste julgeolekuasutuste tööd.**

Militaarse Vastuluureteenistuse seadus (Gesetz über den Militärischen Abschirmdienst, edaspidi: *MADG*) reguleerib Militaarse Vastuluure ülesandeid, volitusi, meetmeid ja tegevust.

Riikliku Luureteenistuse seadus (Gesetz über den Bundesnachrichtendienst (edaspidi: *BNDG*)) reguleerib Riikliku Luureteenistuse ülesandeid, volitusi, meetmeid ja tegevust.

Lisaks nimetatud seadustele reguleerivad julgeolekuasutuste tööd ka eriseadused, kus on ette nähtud järelevalve kord ja protseduurireeglid põhiõiguste riive korral.

Järelevalvet julgeolekuasutuste tegevuse üle reguleerib Riiklike Luureteenistuste Parlamentaarse Kontrolli Seadus (edaspidi: *Kontrollkomisjoni seadus*) (Gesetz über die parlamentarische Kontrolle nachrichtendienstlicher Tätigkeit des Bundes (Kontrollgremiumgesetz)).

Kirjavahetuse, posti ja telekommunikatsiooni privaatsuse riivamise seadus (Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10 Gesetz, G10) edaspidi: *Artikkel 10 seadus*) annab julgeolekuasutustele volitused riivata Saksamaa põhiseaduse artiklist 10 (õigus kirjavahetuse, posti ja telekommunikatsiooni privaatsusele) tulenevaid õigusi. Põhiõiguste riiveid reguleerivad lisaks veel sätted ka BVerfSchG-s, MADG-s ja BNDG-s.

Politsei ja teised korrakaitseasutused on Saksamaal rangelt lahutatud julgeolekuasutustest ning julgeasutustel puuduvad igasugused politseile ja korrakaitseasutustele antud volitused ja meetmed ning õigus politseid ja korrakaitseasutusi oma töös kasutada (BNDG § 1 lg 3, MADG § 1 lg 4 ja BVerfSchG § 8 lg 3). Seega ei ole julgeolekuasutuste volitused ega meetmed reguleeritud Kriminaalmenetluse Seadustikus (StPO) ega teistes sarnastes õigusaktides, mis reguleerivad politsei ja korrakaitseasutuste õigust läbi viia jälitustoiminguid ja töödelda selle käigus kogutud infot.

8.2. Julgeoleku- ja luureasutuste ülesanded, volitused ja meetmed põhiõiguste piiramisel

8.2.1. Julgeolekuasutuste ülesanded

Riiklik Konstitutsioonikaitse Amet - BfV

BVerfSchG kohaselt (§ 1 lg 1) on BfV eesmärgiks kaitsta vaba ja demokraatlikku ühiskonnakorraldust ja selle toimimist ning Saksa riigi ja liidumaade julgeolekut. BVerfSchG kohustab BfV-d tegema koostööd vastava Liidumaa Konstitutsioonikaitse Ametitega (LfV-ga) (BVerfSchG § 1 lg 2) ning pakkuma üksteisele vastastikku tuge ja abi (BVerfSchG § 1 lg 3). Seejuures täidavad Liidumaa

Konstitutsioonikaitse Ametid samu ülesandeid, mis BfV, kuid üksnes liidumaa piires. Lisaks teeb BfV vajadusel koostööd ka teiste Saksamaa julgeolekuasutustega (BND ja MAD).

Riikliku Konstitutsioonikaitse Ameti (BfV) ülesanded on BVerfSchG (§ 3 lg 1) kohaselt järgmised:

1) vaba demokraatliku korra vastaste tegude kohta informatsiooni kogumine ja analüüsimine; riigi või liidumaa julgeolekut ähvardavate tegude kohta informatsiooni kogumine ja analüüsimine; selliste tegude kohta informatsiooni kogumine ja analüüsimine, mis on suunatud ebaseaduslikult konstitutsiooniliste riigi- või liidumaa asutuste või nende liikmete töö takistamisele;
2) informatsiooni kogumine ja analüüsimine välisvõimu nimel tehtava luuretegevusega (vastuluure);
3) selliste tegude kohta informatsiooni kogumine ja analüüsimine, mis vägivallaga või sellega ähvardamisega panevad ohtu Saksamaa Liitvabariigi välishuvid;
4) selliste tegude kohta informatsiooni kogumine ja analüüsimine, mis on suunatud rahvusvaheliste põhimõtete (Saksamaa põhiseaduse § 9 lg 2 tähenduses) vastu, eriti selliste tegevuste kohta, mis on suunatud rahumeelse rahvusvahelise kooseksistentsi vastu (Saksamaa põhiseaduse § 26 lg 1 tähenduses);

Lisaks sellele on BfV ülesanneteks veel julgeolekukontrollis ja tehnilise ohutuse kontrollis osalemine ning avalikkuse teavitamine.

BVerfSchG § 3 lg 2 järgi on BfV ja LfV-d kohustatud tegema koostööd järgmistel juhtudel:

1) julgeoleku kontrolli teostamisel isikute üle, kellele on usaldatud sellised faktid, esemed või teave, mida tuleb hoida salajasena;
2) tehnilise ohutuse kontrolli teostamisel isikute üle, kes töötavad „tundlikel aladel“ (nt isikud, kes töötavad riigisaladuste- või salastatud infoga, ja isikud, kellel on salastatud infole juurdepääs);
3) tehniliste ohutusmeetmete osas kaitsmaks fakte, esemeid ja teavet, mida tuleb hoida salajasena ning nii, et neid ei avaldataks ühelegi kõrvalisele isikule;
4) teistel seaduses ettenähtud juhtudel isikute kontrollimiseks.

Avalikkuse teavitamine. BfV on kohustatud hoidma Saksamaa avalikkust teadlikuna võimalikest ohtudest Saksamaa demokraatlikule süsteemile. BVerfSchG § 16 lõige 1 kohustab BfV-d teavitama avalikkust § 3 lõikes 1 sätestatud tegevustest, juhul kui selleks on piisavalt kaalukad tõendid. BVerfSchG § 16 lõike 2 kohaselt koostab BfV avalikkuse teavitamiseks vähemalt korra aastas raporti. Seejuures on lubatud ka isikuandmete avaldamine, kui nende avaldamine on vajalik konteksti või organisatsioonide või organiseerumata gruppide mõistmiseks ning avalik huvi on suurem kui vastavate isikute huvid (§ 16 lg 3).

Täpsemalt (eristamaks BfV ülesandeid MAD omadest) keskendub BfV oma ülesannetes järgmistele tegevusvaldkondadele:

1) poliitiliselt motiveeritud (nt parem- ja vasakäärmuslusega seotud) kuritegude vastu võitlemine ja nendega seoses info kogumine;
2) välismaalaste islamiterrorismiga ja teiste äärmuslike liikumistega seonduvate tegevuste, millega ohustatakse riigi julgeolekut, vastu võitlemine ja nendega seonduva info kogumine;
3) luure, sh küber- ja tööstusluure;
4) saientoloogiliste organisatsioonide vastu võitlemine ja nende kohta info kogumine.

Militaarne Vastuluure – MAD

MAD-i eesmärk on koguda ja analüüsida informatsiooni, eriti faktilisi ja isiklikke andmeid, luureandmeid ja dokumente, mis on MADG (§ 1 lg 1) kohaselt seotud:

1) jõupingutustega vaba ja demokraatliku korra vastu, riigi või liidumaa julgeoleku säilimise vastu;
2) tegevustega, mis kujutavad ohtu rahvuslikule julgeolekule või spionaažitegevustega välisvõimu nimel.

Seejuures peavad nimetatud tegevused olema suunatud Kaitseministeeriumi personali, asutuste või osakondade vastu ning toime pandud isikute poolt, kes on Kaitseministeeriumi või selle asutuste töötajad või liikmed või keda kahtlustatakse eelnevalt toodud loetelus nimetatud tegevustes osalemises.

Samuti vastutab MAD MADG kohaselt (§ 1 lg 1) sellise informatsiooni (eriti isikuandmete, muude asjakohaste andmete, luureandmete ning dokumentide) kogumise ja analüüsimise eest, mis on seotud Kaitseministeeriumi valitsusala liikmete ja ministeeriumi töötajate ja tulevaste töötajate osalemisega sellistes tegevustes, mis on suunatud rahvusvaheliste põhimõtete vastu (põhiseaduse § 9 lg 2) ning eriti sellistes tegevustes, mis on suunatud rahvuste rahuliku kooseksisteerimise vastu (põhiseaduse § 26 lg 1).

Teatud juhtudel võib MAD oma ülesannete täitmiseks talle antud volitusi kasutada ka isikute suhtes, kes ei ole Kaitseministeeriumi valitsemisala liikmed või töötajad (MADG § 2 lg 1 ja 2).

Hinnates Kaitseministeeriumi valitsemisalas olevate asutuste ja käitiste ning liitlasvägede asutuste ja käitiste ja rahvusvaheliste sõjaliste peakorterite julgeolekusituatsiooni (kui Saksamaa Liitvabariik on võtnud rahvusvaheliste lepingutega kohustused tagada nende asutuste ja käitiste julgeolek ning kui julgeoleku hindamine on antud MAD pädevusse Kaitseministeeriumi ja kõrgeima riigiasutuse vahelise lepinguga), on MAD-i pädevuses analüüsida informatsiooni ning luureandmeid MADG §-s 1 sätestatud tegevuste ja jõupingutuste osas, mis on suunatud nimetatud asutuste ja käitiste vastu. Seda olenemata sellest, kas vastavad tegevused või jõupingutused on läbi viidud isikute poolt, kes on Kaitseministeeriumi valitsemisala töötajad või liikmed (MADG § 1 lg 2).

Lisaks eelnevale on MAD kaasatud julgeolekukontrolli tegemisse ning tehniliste turvameetmete tagamisse (MADG § 1 lg 3).

Julgeolekukontroll. MAD teostab julgeolekukontrolli isikute üle, kes on Kaitseministeeriumi valitsemisala töötajad või tulevased töötajad ning:

1) kellele on usaldatud avalikes huvides tundlikud andmed, materjal või teave; kellele soovitakse vastav ligipääs anda või kes vastava ligipääsu tulevikus saavad;
2) kes on tulevikus Kaitseministeeriumi valitsusalas töötajad tundlikel positsioonidel (MADG § 1 lg 3).

Tehnilised turvameetmed. MAD tagab tehnilised turvameetmed Kaitseministeeriumi valitsusalas läbiviidavate juurdepääsuloata sisenemiste vastu, et kaitsta avalikkuse huvides tundlikuks märgitud fakte, materjali ning teavet.

MADG (§ 3) alusel on MAD-l ja BfV-l kohustus teha omavahel tihedat koostööd ning pakkuda üksteisele abi. Lisaks sellele on BfV-l võimalik laiendada enda meetmete kasutamist BVerfSchG § 3 lõikes 1 sätestatud ülesannete täitmiseks MAD-iga kokku leppides ka isikutele, kes on Kaitseministeeriumi valitsemisala töötajad või liikmed ja langevad MAD-i jurisdiktsiooni, kui konkreetne olukord seda nõuab (MADG § 3 lg 2). Seda siiski ainult juhul, kui esinevad reaalsed viited, et vastavad isikud teevad koostööd isikutega, kes langevad BfV jurisdiktsiooni BVerfSchG § 3 lõikes 1 sätestatud jõupingutuste või tegevustega läbiviimisel ning edasine uurimine oleks teisiti ohus või on võimalik üksnes ülemäärase pingutusega (MADG § 3 lg 2).

Riiklik Luureteenistus - BND

BND allub vahetult Riigikantseleile ja on üldiselt ainus julgeolekuasutus Saksamaal, millel on õigus teha välisluuret BNDG (§ 1 lg-d 1 ja 2, § 12) kohaselt. Välisluure puhul kogub ja analüüsib BND infot, mis on oluline Saksamaa välis- ja julgeolekupoliitika seisukohalt (BNDG § 1 lg 2).

BND ülesanneteks on BNDG § 2 lõike 1 kohaselt koguda ja töödelda informatsiooni:

1) enda personali, asutuste, esemete ja riigi julgeolekuga seoses tundliku informatsiooni või luureallikate kaitseks;
2) isikute kohta, kes töötavad BND-s või selle kasuks, et tagada julgeolekuasutuste turvalisus;
3) mille kontrollimine on vajalik BND eesmärkide täitmiseks;

4) sündmuste kohta välisriikides, mis on nii Saksamaa välis- kui ka sisejulgeoleku tagamiseks olulised, aga seda ainult juhul kui sellist informatsiooni ei ole võimalik muul viisil koguda ja ükski teine asutus pole sellise informatsiooni kogumise eest vastutav.

BND luureobjektid määratletakse valitsuse tegevuskavaga. Hetkel on tegevuskava võtnud fookusesse tuumarelvade leviku, rahvusvahelise terrorismi, kokku varisenud riigid ja konfliktid maavarade üle.[168] Prioriteetsed regioonid on hetkel Lähis- ja Kesk-Ida, Põhja-Aafrika ning Ida- ja Kesk-Aasia.[169]

8.2.2. Riikliku Konstitutsioonikaitse Ameti volitused ja meetmed

Riikliku Konstitutsioonikaitse Ameti (BfV) volitused ja meetmed on sätestatud BVerfSchG-s. BVerfSchG alusel (§ 8 lg 1) on BfV volitatud koguma, töötlema ja kasutama informatsiooni (sh isikuandmeid), mis on tema ülesannete täitmiseks vajalikud seni kuni see ei lähe vastuollu Riikliku Andmekaitse seadusega või vastavate sätetega BVerfSchG-s.

Seejuures võib BfV taotleda üksnes selliste isikuandmete edastamist, milleta ei ole võimalik informatsiooni saada. Seejuures sätestab BVerfSchG § 8 lg 1 olulise eelduse, et andmesubjekti õiguspäraseid huve võib kahjustada üksnes vältimatus ulatuses.

Pärast Pariisi ja Istanbuli terrorismiakte on paljusid õigusakte muudetud selleks, et paraneks informatsiooni jagamine riigisiseste ja teiste riikide julgeolekuasutuste vahel, kes võitlevad rahvusvahelise terrorismiga. Muudatustega loodi ühine andmebaas BfV-le ja teiste riikide julgeolekuasutustele ning laiendati BND volitusi.

BVerfSchG (§ 8 lg 2) sätestab BfV kasutuses olevad meetmed. BVerfSchG § 8 lg 2 annab BfV-le õiguse kasutada salajaseks informatsiooni kogumiseks järgmisi meetmeid, materjale ning instrumente:

1) usaldusisikute ja teavitajate kasutamine;
2) jälgimine;
3) pildi ja heli salvestamine;
4) võltsitud dokumentide ja võltsitud lubade (näiteks teenistusmärgid ning auto numbrimärgid) kasutamine.

Ka meetmete puhul on BVerfSchG § 8 lõikes 2 sätestatud, et informatsiooni hankimine ei tohi olla ebaproportsionaalne võrreldes uuritava fakti olulisusega. Samuti täpsustatakse BVerfSchG § 8 lõike 2 kohaselt vastavad meetmed asutusesiseses dokumendis, mille peab heaks kiitma Siseministeerium, kes teavitab sellest omakorda Parlamentaarset Kontrollkomisjoni.

Juhul, kui andmesubjekti kohta kogutakse teavet selliselt, et andmesubjekt on sellest teadlik, tuleb andmesubjekti teavitada uurimise põhjustest ning andmesubjektile tuleb anda teada, et informatsiooni andmine on andmesubjekti jaoks vabatahtlik (BVerfSchG § 8 lg 4).

Samuti, kui samaaegselt on kohased mitu meedet, peab BVerfSchG (§ 8 lg 5) järgi BfV valima nende seast sellise, mis kõige vähem andmesubjekti kahjustab. Samuti ei tohi valitud meede olla BVerfSchG kohaselt (§ 8 lg 5) andmesubjekti kahjustav põhjusel, et see on saavutatava tulemuse kõrval selgelt ebaproportsionaalne.

Lisaks üldistele meetmetele võib BfV üksikjuhtumite puhul, kui see on vajalik BfV kohustuste täitmiseks, nõuda informatsiooni teleteenuse osutajatelt nende andmetega seonduvalt, mida on talletatud teleteenuste osutamiseks sõlmitud lepinguga, selle tingimustega, muudatuste või lõpetamisega (BVerfSchG § 8a lg 1).

[168] Auftragsprofil der Bundesregierung [Mission Statement of the Federal Government], Bundesnachrichtendienst [Federal Intelligence Service], http://www.bnd.bund.de/DE/Auftrag/Aufgaben/Auftragsprofil_der_Bundesregierung/Auftragsprofil_node.html (01.11.2016)
[169] Ibid.

Üksikjuhtumite puhul on BfV-l täiendavad õigused küsida informatsiooni järgnevatelt asutustelt ja nendega seotud isikutelt (BVerfSchG § 8a lg 2):

1) lennufirmadelt ja arvutipõhiste broneerimissüsteemide operaatoritelt;
2) krediidiasutustelt, finantsasutustelt, rahandusettevõtetelt, kontoomanikelt ja teistelt kasusaajatelt, sh teistelt isikutelt, kes on maksete ja rahade liikumistega seotud;
3) telekommunikatsiooniteenuste osutajatelt liiklusandmete osas;
4) teleteenuste osutajatelt.

Samuti on BfV volitatud küsima üksikjuhtude puhul informatsiooni ka Föderaalselt Keskmaksuametilt (BVerfSchG § 8a lg 2a). Seda siiski ainult juhul, kui see on informatsiooni kogumiseks ja analüüsimiseks vajalik ning kui asjaolud viitavad sellele, et on tõsine oht § 3 lõikes 1 sätestatud huvidele.

Siiski ei ole vastavaid meetmeid võimalik kasutada kõikide isikute vastu. Vastavaid § 8a lõigetes 2 ja 2a sätestatud meetmeid on lubatud kasutada üksnes teatud isikute suhtes BVerfSchG § 8a lg-s 3 sätestatud juhtudel.

BVerfSchG § 8b lg 1 kohaselt peab § 8a lõigetes 2 ja 2a sätestatud meetmete kasutamiseks taotlema luba BfV juht või tema asendaja. Taotlus loa saamiseks peab olema seejuures kirjalik ning põhjendatud. Loa väljastab Siseministeerium.

Load, mis on tulevikus tekkiva informatsiooni avaldamiseks, antakse maksimaalselt kolmeks kuuks (§ 8b lg 1). Juhul kui loa andmiseks vajalikud asjaolud on veel asjakohased, võib vastavat luba pikendada mitte rohkem kui kolmeks kuuks.

Siseministeerium peab igakuiselt teavitama G10 Komisjoni, kes teostab julgeoleku- ja luureasutuste üle järelevalvet, igast loast, mis antakse seoses § 8a lõigetes 2 ja 2a toodud meetmete kasutamiseks, enne loa jõustamist. Ilmse ohu korral võib minister anda korralduse nende lubade kasutamiseks enne Komisjoni teavitamist (BVerfSchG § 8b lg 2). BVerfSchG kohaselt (§ 8b lg 1) hindab G10 Komisjon informatsiooni saamiseks esitatud taotluste vastuvõetavust ja vajalikkust *ex officio* või kaebuste alusel. Siseministeeriumi antud load sellise informatsiooni osas, mida G10 Komisjon peab vastuvõetamatuks või ebavajalikuks, tuleb Siseministeeriumil koheselt tühistada. Sellisel juhul on täiesti keelatud saadud informatsiooni kasutada ning vastavad andmed tuleb koheselt kustutada.

Siseministeerium on kohustatud teavitama Parlamentaarset Kontrollkomisjoni iga kuue kuu tagant nende lubade puhul, mis on väljastatud § 8a lõigete 2 ja 2 a alusel, vastava perioodi jooksul kasutatud meetmetest, meetmete mahust ja ulatusest, kestvusest, tulemustest ning tegevuse maksumusest. Parlamentaarne Kontrollkomisjon on omakorda kohustatud esitama raporti Parlamendile igal aastal meetmete rakendamisest, meetmete olemusest, ulatusest ja põhjustest (BVerfSchG § 8b lg 3).

Seejuures tuleb vastavad load BVerfSchG kohaselt (§ 8b lg 4) esitada isikule, kes on kohustatud informatsiooni esitama kirjalikult sellises mahus, mis on vajalik võimaldamaks isikul oma kohustusi täita. Informatsiooni edastamiseks kohustatud isik ei või andmesubjekte ega kolmandaid isikuid teavitada lubadest ega edastatud informatsioonist.

BVerfSchG § 8a lõikes 1 ja 2 nimetatud asutused peavad edastama informatsiooni ilma viivituseta, täies mahus, korrektselt ja konkreetses § 8-le vastavas vormis (BVerfSchG § 8b lg 6).

BVerfSchG § 9 lg 1 kohaselt võib BfV andmete, sh isikuandmete kogumiseks kasutada BVerfSchG § 8 lõikes 2 sätestatud meetmeid juhtudel, kui asjaolud annavad põhjust arvata, et:

1) sellisel viisil saab teavet § 3 lõikes 1 viidatud jõupingutuste või tegevuste kohta või selle tulemusel saadakse allikas, mis on vajalik sellise teabe uurimiseks;
2) see on vajalik kaitsmaks BfV personali, rajatisi, objekte ja allikaid vaenulike salateenistuste tegevuste või selliste tegevuste eest, mis kujutavad endast ohtu julgeolekule.

Siiski sätestab BVerfSchG § 9 lg 1 erandi ning esimeses punktis toodud informatsiooni kogumine ei ole lubatav, kui faktide ja asjaolude uurimine on võimalik ka andmesubjekti õigusi vähem piiravamal viisil. Üldise reegli kohaselt peetakse piiranguid väiksemateks kui informatsioon saadakse üldiselt kättesaadavatest allikatest või informatsioon saadakse prokuratuurilt, politseilt või teistelt asutustelt.

BVerfSchG § 8 lõikes 2 nimetatud meetmete kasutamine ei tohi olla arusaadavalt ebaproportsionaalne uuritava asja tähtsuse suhtes. Meetme kasutamine tuleb lõpetada niipea, kui selle kasutamise eesmärk on täidetud või kui on indikatsioonid, et eesmärki ei saa üldse saavutada või ei saa eesmärki saavutada vastava meetme kasutamisega (§ 9 lg 2).

BVerfSchG § 9 lõike 2 kohaselt võib privaatvestluste tehnilist pealtkuulamist või salajast lindistamist läbi viia, pilte või videolindistust teha isiku elukohas üksikjuhtumitel üksnes siis, kui see on vajalik hoidmaks ära vahetut üldist ohtu või vahetut ohtu üksikisiku elule ning kui politsei ei suuda sellel hetkel õigushuvisid adekvaatselt kaitsta. Nende meetmete kasutamiseks võib korralduse anda BfV juht või tema asetäitja juhul, kui selleks ei saada õigeaegselt kohtuotsust. Sellisel juhul peab vastava otsuse taotlema kohalikult BfV asukohas olevalt piirkonnakohtult (*Amtsgericht*) ilma viivituseta.

Lisaks on BfV volitatud BVerfSchG § 9 lõike 4 kohaselt kasutama tehnilisi vahendeid, tuvastamaks aktiivselt kasutatava mobiiltelefoni või raadiotelefoni terminali asukohta või konkreetse seadme või kaardi numbri, kooskõlas § 8 lõikega 2. Siiski on selliste tehniliste vahendite kasutamine lubatud üksnes sellistel juhtudel, kui seadme või kaardi numbri tuvastamine ilma tehniliste vahendite kasutamiseta ei ole võimalik. Samuti ei ole lubatud sellise meetme kasutamine kõikide isikute puhul. BVerfSchG § 9 lõige 4 määratleb, et meedet võib kasutada üksnes isikute vastu, kellele on viidatud § 8a lõike 3 punktides 1 ja 2b. Kolmandate isikute suhtes võib selliselt meedet kasutada üksnes juhul, kui soovitava tulemuse saavutamiseks on see tehnilistel põhjustel vältimatu. Siiski on selliste andmete kogumise järel nende kasutamine täielikult keelatud ning need tuleb viivitamatult kustutada.

BVerfSchG § 9a sätestab, et BfV võib omaenda töötajaid (varjatud personal) kasutada, selgitamaks välja BVerfSchG § 3 lõikes 1 sätestatud tegevused ja jõupingutused. Seejuures on § 3 lõike 1 punktides 1 ja 4 sätestatud jõupingutuste väljaselgitamiseks isikute püsiv kasutamine lubatud üksnes juhul, kui jõupingutused on märkimisväärse tähtsusega, eriti kui need on suunatud jõu või vägivalla kasutamisele.

BfV ei tohi BVerfSchG § 9a lõike 1 kohaselt varjatud töötajaid kasutada § 3 lõike 1 punkti 1, 3 või 4 sätestatud püüdluste loomiseks või selliste jõupingutuste mõjutamiseks. Varjatud töötajad võivad gruppides, sh kriminaalsetes gruppides osaleda selleks, et välja selgitada vastavate gruppide kavatsused. Lisaks on selliste kavatsuste elluviimisel lubatud osaleda juhul kui:

1) sellega ei rikuta isiku õigusi;
2) töötajate osalemine kavatsuste elluviimisel on eelduslikult hädavajalik informatsiooni saamiseks;
3) see ei ole väljaselgitatavate asjaoludega võrreldes ebaproportsionaalne.

Olukorras, kus on piisavalt tõendeid, et varjatud töötajad on ebaseaduslikult toime pannud sisulise tähtsusega kuriteo, tuleb missioon koheselt lõpetada ning teavitada õiguskaitseasutust (BVerfSchG § 9a lõige 3).

Lisaks enda töötajate kasutamisele kohaldub BVerfSchG § 9a ka selliste usaldusisikute kasutamisele, kelle koostöö BfV-ga on kolmandatele isikutele teadmata. Seejuures on BfV kohustatud esitama vähemalt korra aastas Parlamentaarsele Kontrollikojale raporti usaldusisikute kasutamisest (BVerfSchG § 9b lg 1). Eeldused, milliseid isikuid BfV usaldusisikutena kasutada ei tohi, on sätestatud § 9b lõikes 2.

8.2.3. Militaarse Vastuluure volitused ja meetmed

Militaarse Vastuluure (MAD) volitused ja meetmed on sätestatud MADG-is ning on sarnased BfV volituste ja meetmetega. Volituste ja meetmete osas teebki MADG viiteid BVerfSchG-le.

MAD võib MADG alusel (§ 4 lg 1) koguda, töödelda ning kasutada informatsiooni (sh isikuandmeid), mis on tema ülesannete täitmiseks vajalikud ning kooskõlas BVerfSchG § 8 lõigetega 2, 4 ja 5 ning kui Riiklik Andmekaitse seadus või vastavad sätted MADG-st seda ei keela.

MAD-il ei ole lubatud koguda isikuandmeid, et täita enda MADG § 1 lõikes 2 sätestatud funktsiooni (julgeolekusituatsiooni hindamine).

BVerfSchG § 8 lg 2 lausetes 2 ja 3 sätestatud meetmed on kasutatavad ka MAD poolt (MADG § 4a). Seejuures annab heakskiidu administratiivsetele juhistele Kaitseministeerium.

Samuti kohaldub MAD tegevusele BVerfSchG § 8a ja 8b, seejuures vaid selle erisusega, et reaalsed viited peavad olema MADG § 1 lõikes 1 sätestatud õiguste ohustamisele (vaba ja demokraatliku korra, riigi või liidumaade julgeolu vastased teod) ning Siseministeeriumi asemel annab heakskiidu asutusesisesele dokumendile Kaitseministeerium.

MAD võib koguda andmeid ja eriti isikuandmeid kooskõlas BVerfSchG §-ga 9 ulatuses, mis on vajalik:

1) MADG § 1 lõikes 1 ja § 2 lõikes 1 sätestatud funktsioonide täitmiseks ning selleks vajalike allikate otsimiseks;
2) kaitsmaks MAD personali, käitisi, vara ning allikaid rahvuslikule julgeolekule ohtu kujutavate tegude vastu või spionaaži tegevuste vastu, sh § 2 lõikes 2 sätestatud tegevused.

MAD tegevusele kohalduvad ka BVerfSchG § 9 lõiked 2-4, mis käsitlevad salajast pealtkuulamist, eravestluste lindistamist, piltide tegemist ning filmimist isiku kodus. Samuti on MAD volitatud kasutama BVerfSchG § 9a lõigetes 2 ja 3 ning §-s 9b sätestatud meetmeid (MADG § 5).

Samuti on MAD volitatud küsima oma ülesannete täitmiseks vajalikku informatsiooni (sh isikuandmeid) kõikidelt teistelt asutustelt ja kontrollima ametlikke registreid (MADG § 10 lg 2).

MAD kogub peamiselt siseriiklikku informatsiooni, kuid erandina on MAD-il õigus koguda ja analüüsida Riikliku Kaitseväe erilise välisülesande või humanitaarmissiooni käigus (MADG § 14 lg 1) andmeid, eriti isikuandmeid ja asjakohast informatsiooni, teavet ning dokumente, mis on vajalikud tagamaks jõudude valmisolek või kaitsmaks Kaitseministeeriumi valitsemisalas olevat personali ja nende perekonna liikmeid, Kaitseministeeriumi käitisi ja asutusi.

Selline informatsioon kogutakse ja analüüsitakse Saksamaal, misjärel info edastatakse militaarasutustele ja organisatsioonidele. Kui sellise missiooni käigus on vaja koguda informatsiooni, siis kaasatakse sellise info kogumisse BND (MADG § 14 lg 2), kes vastavat tegevust läbi viib. Mõlemad asutused sõlmivad omavahel kokkuleppe info kogumise ja töötlemise kohta (MADG § 14 lg 6).

Lisaks on MAD volitatud analüüsima erilise välismissiooni jooksul informatsiooni ka selliste isikute ja isikugruppide kohta, kes ei ole Kaitseministeeriumi valitsemisalas olevad liikmed ega töötajad, kui nende isikute tegevused või jõupingutused on suunatud valitsusala personali, käitiste või asutuste vastu (MADG § 14 lg 2). Kui vastava informatsiooni kogumine on lõike 1 kohaselt oluline, palub MAD BND-l vastava tegevuse läbi viia (MADG § 14 lg 2).

Enne MAD kaasamist sellisele erimissioonile tuleb teavitada ka Parlamentaarset Kontrollkomisjoni (MADG § 14 lg 7). Muudel juhtudel on välise informatsiooni kogumine ja töötlemine MAD-l keelatud (MADG § 14 lg 1 lause 3).

Tulenevalt sellest, et BVerfSchG reguleerib julgeolekuasutuste meetmeid üldosa seadusena, on kõikidel julgeolekuasutustel õigus kasutada samu meetmeid, kuid mõningate piirangutega, mis on seotud julgeoleku asutuse eesmärkidega ja täidetavate ülesannetega. Seega on MAD poolt kasutatavad meetmed eelnevalt kirjeldatud BfV meetmetega samad (MADG § 4 lg 1) ning neid ei hakata käesoleval juhul kordama.

8.2.4. Riikliku Luureteenistuse volitused ja meetmed

Riikliku Luureteenistuse (BND) volitused ja meetmed on sarnased Riikliku Konstitutsioonikaitse Ameti ja Militaarse Vastuluurega, selle erisusega, et kui BfV ning MAD koguvad siseriiklikku informatsiooni, siis BND keskendub välise julgeoleku tagamisele.

BND võib BNDG (§ 2 lg 1) kohaselt koguda, töödelda ja kasutada informatsiooni (sh isikuandmeid), mis on vajalikud tema ülesannete täitmiseks, seni kuni see ei lähe vastuollu Riikliku Andmekaitse Seaduse või BNDG vastavate sätetega. Lisaks sellele on BND-l sarnaselt BfV-ga volitus vahetada teiste asutustega informatsiooni.

Üksikutel juhtudel võib BND selleks, et täita enda ülesandeid, koguda informatsiooni BVerfSchG §-ide 8a 8b alusel (BNDG § 2a). Informatsiooni võib BVerfSchG §-de 8a ja 8b alusel koguda juhul kui:

1. see on vajalik BNDG § 1 lõikes 2 sätestatud ülesannete täitmiseks;

2. kaitsmaks enda töötajaid, asutusi, esemeid ja allikaid ohtlike tegevuste või luuretegevuse eest.

Seejuures kohaldatakse BVerfSchG § 8a lõikeid 2 ja 2a sellisel eeldustel, et seal viidatud § 3 lõikes 1 kaitstavad huvid asendatakse nii, et esinema peavad reaalsed viited Artikkel 10 seaduse § 5 lg 1 lause 3 punktides 1-4 ja 6 sätestatud kaitstavate huvide ohustamisele. Seejuures kohaldatakse BVerfSchG § 8b lõikeid 1-9 üksnes sellise erisusega, et Siseministeeriumi asendab Riigikantselei.

BVerfSchG § 8a lõigetes 2 ja 2a sätestatud meetmeid võib BND kasutada üksnes isikute vastu, kelle puhul on kahtlus, et nad võivad osaleda lõike 1 lauses 2 sätestatud riski loomises või säilitamises ning sellele viitavad otsesed tõendid (BNDG § 2a lg 2).

Samuti on BND volitatud küsima BND ülesannete täitmiseks vajalikku informatsiooni (sh isikuandmeid) kõikidelt teistelt asutustelt ja kontrollima ametlikke registreid (BNDG § 2a, § 8 lg 3). BND võib kasutada salajasi meetmeid, varustust ja seadmeid andmete kogumiseks, kui see on vajalik tema ülesannete täitmiseks.

Tulenevalt sellest, et BVerfSchG reguleerib julgeolekuasutuste meetmeid üldosa seadusena, on kõikidel julgeolekuasutustel õigus kasutada samu meetmeid, kuid mõningate piirangutega, mis on seotud julgeoleku asutuse eesmärkidega ja täidetavate ülesannetega. Seega on ka BND volitatud kasutama BVerfSchG § 8 lõikes 2 sätestatud meetmeid salajaseks informatsiooni kogumiseks, kui see on vajalik BND ülesannete täitmiseks. Samuti on BND-l BVerfSchG §-des 9, 9a ja 9b sätestatud meetmete kasutamise volitus (BNDG § 3).

Siiski peab BND sarnaselt BfV-le ja MAD-ile meetmete kasutamisel valima sellise meetme, mis kõige vähem andmesubjekti riivab ning meede ei tohi põhjustada ebasoodsat olukorda, mis oleks soovitud tulemust arvesse võttes selgelt ebaproportsionaalne (BNDG § 2 lg 4).

Lisaks eelnevatele meetmetele kasutavad kõik julgeolekuasutused ka nö tavapärast kättesaadava info kogumist ja töötlemist, nt ajalehed, flaierid, programmid. Samuti osalevad julgeolekuasutuste agendid avalikel üritustel ja küsitlevad inimesi, kellelt on võimalik saada asjakohast informatsiooni (mitteformaalselt, st tavavestluse käigus koos loaga saadud informatsiooni kasutada).

Julgeolekuasutustel on õigus nõuda informatsiooni ka prokuratuurilt, politseiasutustelt, maksuametilt migratsioonibüroolt jt riigiasutustelt, kui on alust arvata, et kogutud informatsioon on vajalik julgeolekuasutuse eesmärke silmas pidades (BVerfSchG § 18 lõiked 1-3a).

Tulenevalt sellest, et julgeolekuasutused on rangelt politseist eraldatud, ei ole julgeolekuasutustel õigust kasutada jõudu või muid politsei volitusi informatsiooni kogumiseks (BVerfSchG § 2 lg 1 lause 3, § 8 lg 3; MADG § 1 lg 4, § 4 lg 2; BNDG § 1 lg 1 lause 2, § 1 lg 3 lause 1).

8.3. Protseduurid põhiõiguste riive õiguspärasuse tagamiseks

Teised eriseadused (BNDG ja MADG) kasutavad Konstitutsioonikaitse Ameti seaduses reguleeritud protseduure viiteliselt (MADG § 4 lg 1; BNDG § 3) selle erisusega, et arvesse võetakse asutuse enda eesmärki ja ülesandeid ning nõusolek andmete kogumiseks ja töötlemiseks tuleb saada ministeeriumilt või asutuselt, kelle all vastav luure- või julgeolekuasutus töötab.

BVerfSchG § 8 lg 1 kohaselt võib BfV nõuda üksnes selliste isikuandmete edastamist, mis on vajalikud informatsiooni saamiseks. Seejuures võib informatsiooni kogumisel, töötlemisel ja kasutamisel isikute õiguspäraseid huvisid kahjustada üksnes vältimatus ulatuses (§ 8 lg 1).

BVerfSchG § 8 lg 5 kohaselt tuleb erinevate meetmete olemasolul julgeolekuasutustel valida selline, mis riivab andmesubjekti õigusi kõige vähem. Meede ei tohi põhjustada kahju seetõttu, et on soovitud tulemust arvesse võttes ebaproportsionaalne. Sama reegel kehtib ka teiste julgeolekuasutuste (MAD JA BND) puhul ning see tuleneb vastavalt MADG § 4 lg 1 ja BNDG § 2 lõikest 4.

Julgeolekuteasutustel on sisuliselt kaks erinevat protseduuri, sõltuvalt sellest, kas kogutav info jääb Saksamaa põhiseaduse § 10 kaitsealasse või mitte. Andmete kogumine ja töötlemine, mis jääb põhiseaduse artikkel 10 kaitsealasse on reguleeritud „Artikkel 10 seaduses“ ja Konstitutsioonikaitse Ameti seaduses (BVerfSchG). Põhiõiguste riive, mis ei puuduta §-i 10, on reguleeritud Konstitutsioonikaitse Ameti seaduses (BVerfSchG).

Artikkel 10-st tulevate õiguste riive

Saksamaa põhiseaduse § 10 lõike 1 kohaselt on kirjavahetus, post ja telekommunikatsioon puutumatu. § 10 lõike 2 kohaselt võib seda vabadust riivata üksnes kooskõlas seadusega. Kui riive tehakse eesmärgiga kaitsta vaba demokraatlikku korda või tagadamaks Saksamaa Liitvabariigi turvalisus, võib seadusega ette näha, et riivest mõjutatud isikut ei pea riivest informeerima ning kohtusse pöördumise asemel lahendavad konkreetse kaasuse parlamendi poolt määratud asutused.

„Artikkel 10 seaduse“ § 10 lg 1 järgi on ainult kõrgeimal vastaval riigivõimul või Liidukantsleri poolt määratud Riiklikul valitsusasutusel õigus lubada selliste meetmete kasutamist, mis piiravad sõnumisaladuse ja vaba sõnumivahetuse õigust (artikkel 10 õigused). See tähendab, et nimetatud õiguste piiramisele võib loa anda julgeolekuasutust haldava ministeeriumi minister (nt BfV-l on selleks siseminister, kellel on ainsana õigus lubada BVerfSchG § 8a lõigetes 2 ja 2a nimetatud meetmete kasutamist).

MAD puhul kehtib sama analoogia, kuid sellise erinevusega, et MAD allub Välisministeeriumile. Seega võib samade meetmete kasutamist lubada siseministri asemel välisminister (MADG § 4a) ning muus osas on meetmete kasutamise võimalused samad.

Protseduurireeglid on täpsustatud BVerfSchG §-s 9. BND-ga seoses on protseduurilised erisätted kirjas BNDG §-s 2a, mis viitab üldiselt BVerfSchG §-dele 8a ja 8b mõningate erisustega, st BND õigus kasutada Konstitutsioonikaitse seaduse §-s 8a nimetatud meetmeid on piiratud BND eesmärkidest ja olemusest tulenevalt. Õigus nõuda piiravate meetmete kasutamist on sellisel juhul Riigikantsleril.

Artikkel 10 seaduse § 10 lg 2 järgi peab luba olema kirjalikus vormis ja peab sisaldama põhjendusi kui ka vastutavat asutust, kes viib vastava jälitustoimingu läbi.

Enne artiklist 10 tulenevate õigusi piirava (riivava) tegevuse täide viimist peab Parlament tegema igakuise ettekande Artikkel 10 komisjonile ja taotlema heakskiitu. Vahetu ohu korral võib piiravad (riivavad) tegevused ellu viia ka ilma heakskiiduta. Vahetu ohu olukorda pole seaduses lahti seletatud ning kohtupraktika on selle koha pealt puudulik – seda on ette heidetud ka Saksamaa julgeolekuasutuste seadustele, mistõttu on oodata 2018. a reforme julgeolekuseaduste osas[170]. Kui on alustatud jälitustoimingutega ilma luba saamata põhjusel, et tegemist on vahetu ohuga, siis tuleb heakskiit saada ilma viivituseta (Artikkel 10 seadus § 15 lg 6).

Teiste õiguste riive

Protseduurireeglid selliste jälitustoimingute läbiviimiseks näeb ette BVerfSchG § 9[171]. Olulisema nõudena on ette nähtud kohtu luba (§ 9 lg 2 üheksas lause), välja arvatud juhul kui tegemist on vahetu ohuga, mille tähendust seaduses täpsustatud ei ole. Sellisel juhul tuleb viivitamatult pärast jälitustoimingute läbiviimist selline luba saada. Kohtu loa saamisel hinnatakse asutuse pädevust, st kas vastav meede on kooskõlas asutuse eesmärkide ja volitusega, ning kas on olemas vähem piiravaid meetmeid, mida saaks vajaliku info kogumisel kasutada (Konstitutsioonikaitse seaduse § 9 lg 1).

Lisaks on ette nähtud veel andmesubjekti teavitamine ning andmesubjektile informatsiooni edastamine.

8.3.1. Andmesubjekti teavitamine

Juhul kui isikuandmed kogutakse andmesubjektilt tema nõusolekul, tuleb kogumise eesmärki täpsustada. Andmesubjektile tuleb selgitada, et ta annab vastavat informatsiooni vabatahtlikult (BVerfSchG § 8 lg 4, MADG § 4 lg 1, BNDG § 2 lg 2). BNDG kohaselt tuleb lisaks eelnevale veel juhul, kui viiakse läbi julgeolekukontrolli BNDG § 1 lg 2 mõttes, andmesubjekti teavitada kohustusest koostööd teha töölepingu või muu lepingu järgi (§ 2 lg 2).

---

[170] „The Court criticized the legal requirements for carrying out covert surveillance measures as too broad and unspecific and held that the norms allowing the transfer of data to third-party authorities and to authorities in third countries lacked sufficient legal restrictions. The provisions that were declared unconstitutional will mainly remain in force, subject to restrictions, up to and including June 30, 2018.“ https://www.loc.gov/law/help/intelligence-activities/germany.php#_ftn14; ptk I, viies lõik.

[171] Vt viide 3; Viited BVerfSchG § 9-le on samades sätetes, kus on ka viited § 8 lõikele 2.

8.3.2. Andmesubjektile informatsiooni edastamine

Üldiselt on julgeolekuasutused kohustatud andmesubjektile tema taotlusel tema kohta säilitatavat informatsiooni jagama, kui andmesubjekt tõestab, et tal on erihuvi küsitava informatsiooni suhtes. Selline informatsiooni jagamine ei hõlma endas siiski andmete päritolu ning andmeid selle kohta, kellele vastavaid andmeid on edastatud (BVerfSchG § 15 lg 3, BNDG § 7, MAD § 9). Siiski on ette nähtud ka rida erandeid, millal informatsiooni kindlasti andmesubjektiga jagada ei saa (BVerfSchG § 15 lg 2). Sellised otsused võtab vastu vastavalt kas BfV, MAD või BND juht või nende poolt määratud töötaja.

Juhul kui andmesubjektile keeldutakse informatsiooni väljastamast, tuleb andmesubjekti teavitada selle õiguslikust alusest ning sellest, et ta võib selle otsuse vaidlustada Andmekaitse voliniku juures (BVerfSchG § 15 lg 4).

8.3.3. Riiklik Konstitutsioonikaitse Ameti volitused ja meetmed andmete töötlemisel ja talletamisel

Konstitutsioonikaitse seaduse § 10 lg 1 järgi võivad julgeolekuasutused töödelda ja talletada informatsiooni, kui:

1) esinevad ilmingud tegevuste osas, mille uurimisse vastaval julgeolekuasutusel (BfV, MAD või BND) on õigus sekkuda vastavalt tema volitustele;
2) see on vajalik uurimaks tegevusi, mida vastaval julgeolekuasutusel on volitused uurida.

Kõik failid ja informatsioon tuleb kustutada, kui selline informatsioon pole enam vajalik julgeolekuasutuste ülesannete täitmisel või kui selliste andmete kogumine oli lubamatu (Konstitutsioonikaitse seaduse § 12 lg 2). BfV-l ja MAD-il on kohustus kontrollida vähemalt viie aasta jooksul korra, kas kogutud informatsioon on vajalik, ning vajadusel kustutada või muuta kogutud andmed (BVerfSchG § 12 lg 3).

Kogutud failide säilitamise korda reguleerib vastava ministri (BfV korral Siseminister; MAD korral välisminister – MADG § 8; BND korral Riigikantsler – BNDG § 6) väljastatud õigusakt, kus sätestatakse toimikute nimetamise, kasutamise, ligipääsu ja üle vaatamise kord (BVerfSchG § 14 lg 1).

Oma ülesannete täitmiseks võib BfV BVerfSchG § 10 lõike 1 kohaselt säilitada, muuta ja kasutada isikuandmeid järgmistel juhtudel:

1) olemas on reaalsed viited BVerfSchG § 3 lõikes 1 kirjeldatud tegevustele (nt vaba demokraatliku korra vastastele tegudele);
2) see on BVerfSchG § 3 lõikes 1 nimetatud tegevuste uurimiseks vajalik;
3) BfV tegutseb BVerfSchG § 3 lõike 2 alusel.

BfV peab seejuures piirama andmete hoidmist ajani, mis on vajalik tema ülesannete täitmiseks (§ 10 lg 3).

Seejuures alaealiste kohta, kes on nooremad kui 14-aastased, võib BfV BVerfSchG § 11 lg 1 kohaselt säilitada, muuta ja kasutada isikuandmeid üksnes siis, kui on reaalsed viited sellele, et alaealine plaanib, paneb toime või on toime pannud Kirjavahetuse, posti ja telekommunikatsiooni privaatsuse riivamise akti § 3 lõike 1 mõistes kuriteo. Alaealiste puhul, kes on nooremad kui 14-aastat, on andmete või informatsiooni säilitamine keelatud. Vanemate kui 16-aastaste isikute kohta on lubatud andmeid säilitada, kuid vastavad andmed tuleb kustutada mitte hiljem kui kahe aasta jooksul kui just ei ole hiljem leitud teavet isiku § 3 lõikele 1 vastavast tegevusest (§ 11 lg 2)

Pärast kahe aasta möödumist tuleb alaealiste kohta säilitatud andmed üle vaadata ning viie aasta möödumisel tuleb andmed kustutada (§ 11 lg 2), kui rohkem teavet § 3 lõikes 1 sätestatud tegevusest ei ole pärast andmesubjekti täisealiseks saamist saadud.

BfV on kohustatud parandama failides oleva ebakorrektse informatsiooni (§ 12 lg 1). Samuti tuleb BfV-l failides säilitatavad isikuandmed kustutada, kui nende säilitamine oli lubamatu või nendes andmetes peituv teave ei ole enam BfV ülesannete täitmiseks vajalik (§ 12 lg 2). Andmeid siiski ei kustutata, kui

on põhjus uskuda, et kustutamine kahjustaks andmesubjekti õiguslikke huvisid. Sellisel juhul andmed blokeeritakse ning neid edastatakse üksnes andmesubjekti nõusolekul (§ 12 lg 2).

BfV on kohustatud konkreetsete juhtude korral kontrollima hiljemalt iga viie aasta tagant, kas säilitatav informatsioon tuleb parandada või kustutada. Isikuandmed, mida säilitatakse § 3 lg 1 punktis 1, 3 ja 4 sätestatud jõupingutuste kohta, tuleb kustutada hiljemalt 10 aasta möödumisel, kui just BfV juht või tema asetäitja ei otsusta erandkorras kindlal juhtumil teisiti (§ 12 lg 3).

Isikuandmed, mida säilitatakse üksnes andmekaitse kontrolliks, andmete hoidmiseks või selleks, et tagada andmehaldamise süsteemi kohane toimimine, võidakse kasutada üksnes nendel eesmärkidel (§ 12 lg 4).

Juhul kui BfV on kindlaks teinud, et salvestistes säilitatavad isikuandmed on valed või kui nende õigsuse on vaidlustanud andmesubjekt, tuleb selle kohta teha salvestisele märge või tuleb see muul moel salvestada (§ 13 lg 1).

BfV-l on kohustus isikuandmed blokeerida, kui BfV poolt on kindlaks tehtud, et kindlatel juhtudel saaksid ilma isikuandmete blokeerimiseta andmesubjekti õiguslikud huvid kahjustada ning andmed ei ole enam tulevikus täidetavate ülesannete täitmiseks vajalikud (§ 13 lg 3). Blokeeritud andmed tuleb ka vastavalt märkida ning neid ei või enam rohkem kasutada ega edastada. Siiski on võimalik ka blokeeringu tühistamine, kui blokeerimise aluseks olevad asjaolud on ära langenud.

8.3.4. Militaarse Vastuluure volitused ja meetmed andmete töötlemisel ja talletamisel

MAD võib MADG (§ 6 lg 1) kohaselt isikuandmeid säilitada, muuta ja kasutada kooskõlas BVerfSchG §-ga 10 ulatuses, mis on vajalik tema ülesannete täitmiseks. Kogutud ja säilitatud andmeid isikute kohta, kes ei ole Kaitseministeeriumi valitsemisala töötajad ega liikmed, ei tohi kasutada muuks kui MAD ülesannete täitmiseks, kui nende kasutamine ei ole just MADG § 1 lg 1 kohaselt keelatud.

MADG kohaselt (§ 6 lg 2) on MAD kohustatud parandama, kõrvaldama ja blokeerima oma failides säilitatavad isikuandmed kooskõlas BVerfSchG § 12-ga.

Alaealiste kohta arvutifailide või dokumendifailidena kogutud andmed vaadatakse kahe aasta möödudes üle selleks, et olla kindel nende säilitamise vajaduses ning sellised andmed kustutakse hiljemalt viie aasta möödumisel (kui just ei ole ilmnenud pärast isiku täisealiseks saamist uut teavet MADG § 1 lg 1 ja § 2 sätestatud tegevuste kohta). Eelnev ei kohaldu, kui isikut uuritakse MADG § 1 lõike 3 alusel. Siiski on keelatud isikuandmete säilitamine nooremate kui 16-aastaste isikute kohta (MADG § 7 lg 2).

8.3.5. Riikliku Luureteenistuse volitused ja meetmed andmete töötlemisel ja talletamisel

BND võib BNDG kohaselt (§ 4 lg 1) säilitada, muuta ning kasutada isikuandmeid kooskõlas BVerfSchG §-ga 10 ulatuses, mis on vajalik tema ülesannete täitmiseks. Seejuures on alaealiste isikuandmete säilitamine, muutmine ja kasutamine lubatav üksnes kooskõlas BVerfSchG §-ga 11 ja olukorras, kus üksikjuhtumi asjaolude järgi ei saa välistada, et alaealine võib kujutada ohtu Saksamaa kodanike eludele või tervisele väljaspool Saksamaad või Saksa institutsioonidele väljaspool Saksamaad (§ 4 lg 2).

BND on kohustatud parandama, kustutama ja blokeerima andmefailides säilitatud isikuandmeid kooskõlas BVerfSchG §-ga 12. BND on kooskõlas BVerfSchG § 12 lg 3 lausega 1 kohustatud kontrollima hiljemalt iga 10 aasta tagant, kas säilitatud andmeid tuleks muuta või kustutada (BNDG § 5 lg 1).

BND on kohustatud parandama ja blokeerima salvestistes säilitatavaid isikuandmeid kooskõlas BVerfSchG §-ga 13 (BNDG § 5 lg 2). Elektrooniliste failide kasutamisel kohaldub BVerfSchG § 13 lõige 4, võttes arvesse, et elektrooniliste failide vajadust ja ülesannete täitmist hinnatakse mitte hiljem kui 10 aasta möödumisel (BNDG § 5 lg 2).

8.4. Järelevalve korraldus julgeoleku- ja luureasutuste tegevuse õigus- ja eesmärgipärasuse üle

Julgeolekuasutused alluvad nii andmekaitse- ja vabaduse voliniku, Parlamentaarse Kontrollkomisjoni kui ka Artikkel 10 Komisjoni järelevalvele.

8.4.1. Parlamentaarne järelevalve

Parlamentaarne Kontrollkomisjon (PKGr)

PKGr on võrreldav Eesti Riigikogu julgeolekuasutuste järelevalve komisjoniga. Saksamaa põhiseaduse § 45d alusel on vastu võetud Riiklike Luureteenistuste Parlamentaarse Kontrolli Seadus (Kontrollkomisjoni Seadus), mille alusel on Parlamentaarne kontrollkomisjon (PKGr) asutatud.

PKGr vaatab üle kõikide eelnevalt nimetatud julgeolekuasutuste tegemised (BfV (ja seoses sellega ka Lfv-de), MAD ja BND). PGKr liikmed määrab Parlament enda liikmete hulgast. Parlament otsustab liikmete arvu, koosseisu ja töömeetodid (Kontrollkomisjoni seaduse § 2). Hetkel koosneb Parlamentaarne Kontrollkomisjon 9 liikmest.[172] PKGr-i arutelud on kinnised (Kontrollkomisjoni seadus § 10).

Järelevalve tulemusena koostab PKGr arvamused ja hinnangud julgeolekuasutuste tegevuse üle, mis kantakse ette valitsusele. Seega on tegemist sisuliselt poliitilise järelevalvega.

Parlament peab Komisjonile avaldama kõikehõlmava informatsiooni riiklike luureteenistuste üldiste tegevuste kohta ja ka informatsiooni tegevuste kohta, mis on olulised Komisjoni ning lisaks ka menetluste jaoks, mis on ette nähtud PKGr-is (Kontrollkomisjoni seaduse § 5).

Komisjon võib saada ka loa siseneda luureteenistuse ja valitsuse vastavatesse valdustesse ning intervjueerida nende liikmeid. Kohtud ja ametnikud on sellises olukorras kohustatud andma õiguslikku ja administratiivset abi (Kontrollkomisjoni seaduse § 5).

Lisaks sätestab seadus spetsiaalsed teavitamise nõuded (vt täpsemalt artikkel 10 seadus § 14, BVerfSchG § 8b lg 3, MADG § 14 lõiked 6 ja 7).

PKGr kannab enda järelevalvetegevusest ette Parlamendile kaks korda valimisperioodi jooksul (poole valimisperioodi jooksul ning valimisperioodi lõpus) (Kontrollkomisjoni seadus § 13). Raportid on avalikult kättesaadavad[173].

Artikkel 10 Komisjon (kasutatakse ka G10 Komisjon)

Saksamaa põhiseaduse artiklist 10 tulenevate õiguste (kirjavahetuse ja telekommunikatsiooni privaatsus) riivamise üle teostab järelevalvet Artikkel 10 Komisjon (Artikkel 10 Seadus § 1 lg 2 ja § 15).

Artikkel 10 Komisjon koosneb neljast liikmest ja need määrab Parlamentaarne Kontrollkomisjon. Komisjoni eesistuja peab kvalifitseeruma kohtuniku ametikohale. Lisaks sellele on Artikkel 10 Komisjonis ka 4 asendusliiget, kes võivad osa võtta koosolekutelt sõnaõiguslikult (st õigus kõneleda ja küsida küsimusi) (Artikkel 10 seadus § 15).

Artikkel 10 Komisjon otsustab *ex officio* või kaebustest tulenevalt, kas kirjavahetuse ja telekommunikatsiooni privaatsuse riived on lubatavad ja vajalikud. Komisjoni pädevuses on kontrollida julgeolekuasutuste poolt Artikli 10 seadusele vastavat isikliku informatsiooni kogumist, töötlemist ja kasutamist (Artikkel 10 seadus § 15 lg 5).

Enne kirjavahetuse ja telekommunikatsiooni privaatsuse riivamist peab vastutav ministeerium raporteerima igakuiselt Artikkel 10 Komisjonile ja taotlema heakskiitu. Juhul, kui on ilmne oht, võib riiveid teostada ilma eelneva heakskiiduta. Heakskiit tuleb saada asjatu viivituseta (Artikkel 10 seadus § 15 lg 6).

Kommentaariks eelnevatele üldistele õigustele: Saksa Konstitutsioonikohus on oma lahendis öelnud, et info, mis puudutab suhtlust välisriikide luureteenistustega, edastamisest ei saa keelduda

[172] http://www.bundestag.de/ausschuesse18/gremien18/pkgr/mitglieder/261126 (01.11.2016).
[173] Viimased rapordid perioodi november 2013 kuni detsember 2015 avaldati 2016. aasta märsis. vt Deutscher Bundestag: Drucksachen und Protokolle [BT-Drs.] 18/7962, http://dipbt.bundestag.de/doc/btd/18/079/1807962.pdf, archived at http://perma.cc/LU7G-PCS7 .

uurimiskomisjoni ees üksnes üldisel põhjendusel, et sellise info jagamine võib kahjustada riigi huvisid.[174] Kohus rõhutas, et keeldumisel peab andma ka konkreetse keeldumise põhjuse.

8.4.2. Andmekaitse ja -vabaduse volinik

Andmekaitse ja -vabaduse volinik jälgib julgeolekuasutuste tegevuse vastavust andmekaitse seadustele – täpsemalt Riikliku Andmekaitse seadusele[175] - aga ka vastavust julgeolekuasutuste tegevust reguleerivates seadustes olevatele täpsustavatele andmekaitse sätetele, nt:

- BVerfSchG §§ 14, 15 ja 22a;
- BVerfSchG §§ 2, 9a ja 10.

Volinikul ei ole õigusi osas, mis puudutab põhiseaduse artikkel 10 õiguste (telekommunikatsiooni, posti ja sõnumivabadus) piiramisega seoses kogutud andmeid, sest selliste andmete kogumise ja töötlemise vastavust seadusele on õigus kontrollida ainult Artikkel 10 Komisjonil (vt eelnevalt ptk 1.4.1. Artikkel 10 Komisjon).

Voliniku määrab ametisse Parlament valitsuse ettepanekul viieks aastaks (Riikliku Andmekaitse seadus §22).

Volinik teostab järelevalvet kogutud info töötlemise talletamise osas. Volinikul on õigus teha ettekirjutusi julgeolekuasutustele, kui info töötlemise ja talletamise reegleid rikutakse (Riikliku Andmekaitse seaduse § 38 lg 5). Volinikul on õigus anda ka sisend julgeolekuasutuste andmete haldamise eeskirja kujundamisel (Konstitutsioonikaitse seaduse § 14 lg 1).

8.5. Julgeoleku- ja luureasutuste volitused ja meetmed elektroonilise side jälgimisel ning andmete töötlemisel ja talletamisel

Teatud ülesannete täitmiseks võib BfV kasutada tehnilisi vahendeid selleks, et tuvastada aktiveeritud mobiiltelefoni terminali asukoht, seerianumbrid ning kaardikoodid. Tehnilisi vahendeid võib kasutada üksnes juhul, kui jälgimise eesmärki ei saa üldse täita või oleks ilma identifitseerimise tegemiseta keerulisem (BVerfSchG § 9 lg 4). Kolmanda isiku isikuandmeid võib koguda selliste meetmete kasutamisel üksnes juhul kui see on viivitamatult tehnilistel põhjustel. Selliste andmete kasutamine on aga rangelt keelatud ning andmed tuleb meetme kasutamise lõpetamisel viivitamatult kustutada. Sama volitus on ka MAD-il ning BND-l.

Üldiselt tulevad julgeolekuasutuste volitused ja meetmed elektroonilise side jälgimiseks Artikkel 10 seadusest, mille § 1 sätestab, et BfV-l, MAD-il ning BND-l on volitus telekommunikatsiooni jälgida ning seda salvestada. BfV, MAD ning BND võivad vastavaid meetmeid kasutada selleks, et ennetada ilmset ohtu vabale ja demokraatlikule korrale, Saksamaa julgeolekule või Saksamaal paiknevate NATO liikmesriikide relvajõududele. BND võib lisaks veel kasutada vastavaid volitusi oma BNDG § 1 lõikes 2 ja § 5 lõike 1 lause 3 punktides 2-6 ja § 8 lõike 1 lauses 1 sätestatud eesmärkide täitmiseks. Seejuures võivad julgeoleku- ja luureasutused, ennetades ilmset ohtu vabale ja demokraatlikule korrale, Saksamaa julgeolekule või Saksamaal paiknevate NATO liikmesriikide relvajõududele avada ja uurida ka saadetisi.

Artikkel 10 seaduse § 2 sätestab, et isikud, kes osutavad postiteenust, on kohustatud pädeva asutuse taotlusel esitama postiteenuse ja neile hoidmiseks, edastamiseks või kohale toimetamiseks usaldatud saadetiste kohta informatsiooni. Isikud, kes osutavad telekommunikatsiooniteenust, on kohustatud pädeva asutuse taotlusel esitama informatsiooni loa jõustumise järgse telekommunikatsiooni kohta,

---

[174] BVerfG, 124 BVerfGE 78, 123 et seq., pressi väljaanne, kus võetakse kohtuotsus lühidalt kokku ka inglise keeles: https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/EN/2009/bvg09-084.html , archived at http://perma.cc/7JJW-SCUC .

[175] Bundesdatenschutzgesetz [Riiklik Andmekaitse seadus], Jan. 14, 2003, BGBl. I at 66, muudetud, http://www.gesetze-im-internet.de/bundesrecht/bdsg_1990/gesamt.pdf , arhiveeritud http://perma.cc/5AH5-8YT2, mitteametlik inglisekeelne tõlge on saadaval at http://www.gesetze-im-internet.de/englisch_bdsg/federal_data_ protection_act.pdf, archived at http://perma.cc/AD3N-DPY3.

samuti esitama vastavale asutusele neile usaldatud saadetised, mis tuleb telekommunikatsioonivahendite abil edastada ning võimaldada asutusel teostada telekommunikatsiooni jälgimist ja salvestamist. Vastav regulatsioon ei mõjuta BVerfSchG § 8a lõikes 2, MADG § 4a ja BND § 2a sätestatut.

Artikkel 10 seaduse § 3 lõikes 1 on sätestatud, milliste kuritegude ja tegevuste plaanimisel või toimepanemisel vastavaid Artikkel 10 §-s 1 sätestatud meetmeid (jälgimine ning salvestamine) kasutada on lubatud. Samuti on Artikkel 10 seaduse §-s des 5 ja 8 toodud, millistel juhtudel võib BND kasutada vastavaid meetmeid rahvusvaheliste telekommunikatsiooni liiklusandmete suhtes. Artikkel 10 seaduse § 5 lõike puhul võib seal toodud ohtude tuvastamiseks BND lõike 2 kohaselt telekommunikatsiooni liiklusandmete osas meetmete kasutamisel teostada üksnes otsingusõnadel põhinevat üldist jälgimist, mis võimaldavad täpsustada vastavas loas kirjeldatud ohuvaldkonnaga seonduvat. § 8 lõike 3 kohaselt võib §-s 8 kirjeldatud juhtudel, kui see on vajalik tuvastamaks ohtu välisriigis viibiva isiku elule või tervisele, kasutada otsingusõnu vaid selleks, et saada teavet loas täpsustatud ohu kohta.

Julgeoleku- või luureasutus, kes andmeid kogub, peab viivitamata ja korrapärase sagedusega, kuid mitte rohkem kui kuue kuu pärast kontrollima, kas kogutud isikuandmed on vajalikud vastava asutuse Artikkel 10 seaduse § 1 lõike 1 punktis 1 toodud eesmärkide saavutamiseks (Artikkel 10 seadus § 4 lg 1, § 6 lg 1). Juhul, kui vastavad andmed ei ole eesmärkide saavutamiseks vajalikud ning neid ei tule ka teistele asutustele edastada, tuleb vastavad andmed viivitamata kustutada. Andmete kustutamise kohta tuleb hoida dokument. Sellistes dokumentides hoitav teave tuleb seejuures kalendriaasta lõpus kustutada.

Juhul kui andmed on vajalikud andmesubjekti teavitamiseks või piirava meetme kasutamise kohtulikuks arutamiseks, on andmete kustutamine keelatud (§ 6 lg 1). Sellisel juhul tuleb andmed blokeerida ning neid võib kasutada üksnes eeltoodud põhjustel (§ 6 lg 1).

Andmed, mida ei kustutata, tuleb tuvastada ning neid andmeid võib kasutada üksnes nendel eesmärkidel, mis on sätestatud Artikkel 10 seaduse § 5 lõike 1 lauses 3 ning § 7 lõigetes 1-4 ning §-s 7a.

BND taotlusel võib kogutud andmeid pädeva ministri loal ja kooskõlas § 10 lõikega 1, kontrollida automatiseeritud protsessis kehtivate telefoninumbrite või muude spetsiaalsete telekommunikatsiooni ühenduste vormide tuvastamiseks (Artikkel 10 § 6 lg 3).

Lisaks võivad BVerfSchG § 8d, MADG § 4b ning BNDG § 2b kohaselt BfV, MAD kui ka BND juhul, kui see on vajalik nende ülesannete täitmiseks, küsida informatsiooni telekommunikatsiooniteenuse osutajalt Telekommunikatsiooniseaduse §-de 95 ja 111 alusel kogutud teabe osas. Juhul kui vastav taotlus informatsiooni edastamiseks seondub andmetega, mis kaitseb ligipääsu terminalidele või terminalides kasutatavatele andmehoidmise seadmetele, võib informatsiooni küsida üksnes juhul, kui on olemas õiguslik alus andmete kasutamiseks.

Andmete säilitamise ja hoidmise kohta on täiendavad protseduurireeglid kirjas BVerfSchG §§ 10-14 üldreeglitena. Erisused eriseadustest tulevad MAD korral MADG §-dest 6-8 ja BND korral BNDG §-dest 4-6.

8.6. Järeldused läbivate üldpõhimõtete kohta julgeoleku- ja luureasutuste tegevuse reguleerimisel ning elluviimisel

Saksamaa julgeoleku- ja luureasutuste tegevuse regulatsiooni iseloomustab hea organiseeritus. Iga julgeolekuasutuse tegevust reguleerib eraldi seadus. BfV puhul BVerfSchG, MAD puhul MADG ning BND puhul BDNG. Siiski on BVerfSchG käsitletav üldosaseadusena, kuna MADG ning BNDG mõlemad viitavad suures osas BVerfSchG-i erinevatele sätetele. Samuti on regulatsioonid loogiliselt üles ehitatud ning sisaldavad endas vajalikke viiteid teistele seadustele.

Regulatsioonidele võib ette heita ebaselgust. Näiteks ei ole piisavalt selgelt sõnastatud, millistel juhtudel julgeolekuasutused vastavaid meetmeid kasutada võivad ning milline täpsemalt on nende meetmete ulatus. Samuti on Militaarse Vastuluure ning Riikliku Luureteenistuse puhul keeruline üksnes nende tegevust reguleeriva seaduse pinnalt aru saada, millised on asutuse volitused ja meetmed ning kuidas on muu tegevus reguleeritud. Selles osas teevad nimetatud õigusaktid palju viiteid BVerfSchG-ile kui üldosaseadusele. Siiski on Saksamaa regulatsiooni puhul võimalik eristada kõikide julgeolekuasutuste

ülesanded, volitused ning meetmed. Kuigi igal julgeolekuasutusel on erinevad ülesanded, on nende volitused ja meetmed üldiselt identsed.

Saksamaa regulatsioon sätestab erinevad meetmed ning protseduurid (*ex ante* kui ka *ex post* järelevalvemehhanismid) julgeolekuasutustele võimaldatud meetmete kasutamisel põhiõiguste riive õiguspärasuse tagamiseks. Regulatsioonidest nähtub, et julgeoleku tagamisel ning muude julgeolekuasutuste ülesannete täitmisel on lubatud kasutada erinevaid meetmeid, mis piiravad isikute põhiõigusi. Samal ajal nähakse ette mitmed üldised põhimõtted, nt vajalikkus ja proportsionaalsus, et isikute põhiõiguseid ei riivataks rohkem kui vajalik. Saksamaa regulatsiooni puhul pööratakse palju tähelepanu põhiõiguste kaitsele ning suuremas osas sätetest, milles julgeolekuasutustele volitus tagatakse, juhitakse tähelepanu ka andmesubjekti põhiõiguste arvestamise vajadusele. Põhiõiguste kaitse ulatust Saksamaa puhul näitab ka erinevate järelevalveasutuste hulk.

Üldiselt on julgeolekuasutused kohustatud andmesubjektile tema taotlusel andmesubjekti kohta säilitatava informatsiooni jagama. Siiski on ette nähtud ka rida erandeid, millal informatsiooni kindlasti andmesubjektiga jagada ei saa.

Seega kokkuvõtlikult lähtub Saksamaa regulatsioon põhimõttest, et julgeoleku kaalutlustel võib isikute põhiõiguseid riivata, arvestades sealhulgas proportsionaalsuse põhimõtet, kuid ei ole üheselt selge, kuivõrd tegelikkuses suudavad *ex ante* ja *ex post* järelevalvemehhanismid põhiõiguste riive õiguspärasust tagada.

8.7. Saksamaa ja Eesti regulatsioonide võrdlus

Eesti ja Saksamaa julgeoleku- ja luureasutuste regulatsioonid on erinevad.

Peamine erinevus seisneb selles, et Eestis reguleerib julgeoleku- ja luureasutuste tegevust tunduvalt rohkem õigusakte ning regulatsioon on üldiselt killustatud. Saksamaal puudub erinevalt Eestist üks õigusakt, kus oleksid sätestatud julgeolekuasutuste ülesanded, volitused ning meetmed. Seejuures Saksamaal on iga julgeolekasutuse jaoks eraldi seadus. Kuigi BVerfSchG on Saksamaal üldosaseadusena käsitletav, ei võimalda seaduse enda tekst seda järeldust teha ning vastavad viited tulevad MAD ja BND tegevust reguleerivatest seadustest.

Samuti on suureks erinevuseks see, et võrreldes Eestiga on Saksamaal julgeoleku- ja luureasutuste tegevus selgelt eraldatud politseifunktsioonidest. Lisaks on erinev ka julgeolekuasutuste arv ning meetmete jaotus. Eestis on julgeolekuasutusi kaks, Saksamaal kolm. Samuti on erinev see, et Eestis on julgeolekuasutustel igal ühel teatud meetmed, mida ainult nemad kasutada võivad, Saksamaal on meetmete ring väga täpselt piiritletud ning neid võivad kasutada kõik julgeolekuasutused.

Sarnane on Eesti ja Saksamaa puhul see, et mõlemas riigis on välisteabe kogumiseks olemas eraldi asutus: Eestis Teabeamet ning Saksamaal Riiklik Luureteenistus ning samuti eristatakse mõlemas riigis sõjalist ja mittesõjalist julgeolekuasutuste tegevust.

Julgeoleku- ja luureasutuste ülesanded, volitused ja meetmed on üldises plaanis sarnased. Erinevusena saab välja tuua selle, et Eesti õigusaktides on oluliselt täpsemalt määratletud julgeolekuasutuste meetmed elektroonilise side ja elektrooniliste seadmete jälgimise jaoks.

Põhiõiguste riive õiguspärasuse tagamiseks sätestatud protseduuride osas on sarnane see, et üldiselt on piiritletud, mille jaoks vastavaid meetmeid on lubatud kasutada. Samuti sarnanevad Eesti ja Saksamaa regulatsioonid selles osas, et mõlemas regulatsioonis peavad julgeolekuasutused lähtuma oma tegevuses põhiõiguste kaitse, proportsionaalsuse ja eesmärgipärasuse põhimõtetest.

Oluline erinevus Eesti ja Saksamaa regulatsioonide vahel seisneb ka selles, et Saksamaal ei ole prokuratuurile antud rolli meetmete kasutamise jaoks loa väljastamiseks.

Saksamaa regulatsioon näeb samuti reeglina ette isiku teavitamise, kuid sellest tehakse erandeid, samuti on Saksamaa regulatsiooni puhul selged reeglid alaealiste kohta kogutava teabe säilitamise kohta, mis Eesti puhul selgelt reguleeritud ei ole.

Järelevalve osas erinevad Eesti ja Saksamaa regulatsioonid selle poolest, et Saksamaal on järelevalve osas peamine rõhk pandud parlamentaarsele kontrollile, mida teostavad kaks asutust. Samuti on

Saksamaal kaasatud järelevalve tegemisse andmekaitse ja -vabaduse volinik, kes jälgib julgeolekuasutuste tegevuse vastavust andmekaitse seadustele. Sellist rolli kannab Eestis õiguskantsler. Lisaks sellele eristab Eestit järelevalve osas Saksamaast ka see, et Eestis teostab julgeolekuasutuste üle järelevalvet prokuratuur, kellel Saksamaal on julgeolekuasutustele üksnes abistav roll (nt informatsiooni edastamiseks).

Julgeoleku- ja luureasutuste volituste ja meetmete osas andmete töötlemisel ja talletamisel on erinev see, et Saksamaa puhul on väga selgelt seaduse tasandil piiritletud, millise ajaperioodi tagant vastav informatsioon üle vaadatakse ning kustutatakse. Samuti on Saksamaa regulatsioonis ette nähtud julgeolekuasutustele selged juhised andmete töötlemise ja kasutamise jaoks.

9. LISA 1: MEETMETE VÕRDLEV TABEL

Riik	Amet	Meede																										
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29
Eesti	Kaitsepolitseiamet	x	x	x	x					x	x	x	x	x	x	x	x	x				x	x	x	x	x	x	x	x	x
	Teabeamet	x	x	x	x			x		x	x	x	x		x	x					x	x	x	x	x					x
	Kaitsevägi				x			x					x	x	x	x	x				x	x		x	x					
Soome	Suojelupoliisi (SUPO)	x	x		x					x	x		x	x	x	x			x	x		x				x	x	x	x	x
	Pääesikunnan Tiedusteluosasto (PVTK)	x	x		x								x			x						x		x						
Rootsi	Säkerhetspolisen (SÄPO)	x	x	x	x								x		x	x	x							x		x	x	x	x	x
	Försvarsmakten Försvarets Radioanstalt (FRA) Försvarets materielverk (FMV) Totalförsvarets forskningsinstitut, (FOI)						x	x					x											x						

1. Teabe salajane pealtkuulamine ja –vaatamine
2. Elektroonilise side pealtkuulamine/vaatamine
3. Postisaadetise läbivaatamine, asendamine, konfiskeerimine
4. Elektroonilise side andmete kogumine
5. Massiline andmete kogumine
6. Massiline elektroonilise side andmete kogumine/ jälgimine
7. Signaalluure
8. Krüpteeritud andmete uurimine
9. Objekti, isiku asukoha tuvastamine
10. Arvutisüsteemi/IT süsteemi sisenemine
11. Pangakontode andmete kogumine
12. Konspiratsioonivõtted, isiku, asutuse, organi teesklemine, variisik, politseiagent
13. Isiku kaasamine salajasele koostööle
14. Ruumi, hoone, sõiduki, asja, isiku läbiotsimine või läbivaatus
15. Isiku, asja või koha varjatud jälgimine
16. Võrdlusmaterjali kogumine, esmauuringute tegemine
17. Kuriteo matkimine
18. Näiliste tehingute tegemine
19. Kontrollitud läbipääs
20. Jälitustoimingud välisriikides
21. Avalik ja eraõiguslikelt isikutelt teabe saamine
22. Avalik ja eraõiguslikelt isikutelt abi nõudmine
23. Juurdepääs riigi andmekogudele
24. Küsitlemine
25. Liikumisvabaduse piiramine
26. Sõiduki peatamine
27. Kinnipidamine/vahistamine
28. Isiku kontrollimine
29. Isiku samasuse tuvastamine

Riik	Amet	Meede																											
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29
Holland	De Algemene Inlichtingen-en Veiligheidsdienst (AIVD)	x	x	x	x			x	x		x		x		x	x					x	x								
	Militaire Inlichtingen-en Veiligheidsdienst (MIVD)	x	x	x	x			x	x		x		x		x	x					x	x								
Saksamaa	Bundesamt für Verfassungsschutz (BfV)	x	x	x	x			x		x	x	x	x	x		x						x	x	x	x				x	
	Der Militärischen Abschirmdienst (MAD)	x	x	x	x			x		x	x	x	x	x		x						x	x	x	x				x	
	Bundesnachrichtendienst (BND)	x	x	x	x			x		x	x	x	x	x		x					x	x	x	x	x					
UK	Security Service (MI5)	x	x	x	x	x	x	x	x		x		x	x	x	x								x						
	Secret Intelligence Service (MI6)	x	x	x	x	x	x	x	x		x		x	x	x	x					x			x						
	Government Communications Headquarters (GCHQ)	x	x	x	x	x	x	x	x		x		x	x	x	x					x			x						

1. Teabe salajane pealtkuulamine ja –vaatamine
2. Elektroonilise side pealtkuulamine/vaatamine
3. Postisaadetise läbivaatamine, asendamine, konfiskeerimine
4. Elektroonilise side andmete kogumine
5. Massiline andmete kogumine
6. Massiline elektroonilise side andmete kogumine/ jälgimine
7. Signaalluure
8. Krüpteeritud andmete uurimine
9. Objekti, isiku asukoha tuvastamine
10. Arvutisüsteemi/IT süsteemi sisenemine
11. Pangakontode andmete kogumine
12. Konspiratsioonivõtted, isiku, asutuse, organi teesklemine, variisik, politseiagent
13. Isiku kaasamine salajasele koostööle
14. Ruumi, hoone, sõiduki, asja, isiku läbiotsimine või läbivaatus
15. Isiku, asja või koha varjatud jälgimine
16. Võrdlusmaterjali kogumine
17. Kuriteo matkimine
18. Näiliste tehingute tegemine
19. Kontrollitud läbipääs
20. Jälitustoimingud välisriikides
21. Avalik ja eraõiguslikelt isikutelt teabe saamine
22. Avalik ja eraõiguslikelt isikutelt abi nõudmine
23. Juurdepääs riigi andmekogudele
24. Küsitlemine
25. Liikumisvabaduse piiramine
26. Sõidukipeatamine
27. Kinnipidamine/vahistamine
28. Isiku kontrollimine
29. Isiku samasuse tuvastamine

10. LISA 2: PROTSEDUURIDE VÕRDLEV TABEL

Riik	Amet	Protseduurid						
		Kohtu luba	Ministri luba	Prokuratuuri luba	Ameti juhi luba	Ametniku otsus	Juristi osalemine menetluses	Isiku teavitamine
Eesti	Kaitsepolitseiamet	x	x	x	x	x		x
	Teabeamet	x	x		x	x		x
	Kaitsevägi		x	x	x	x		x
Soome	Suojelupoliisi (SUPO)	x			x	x	x	x
	Pääesikunnan Tiedusteluosasto (PVTK)	x			x	x		x
Rootsi	Säkerhetspolisen (SÄPO)	x		x	x	x	x	
	Försvarsmakten Försvarets Radioanstalt (FRA) Försvarets materielverk (FMV) Totalförsvarets forskningsinstitut, (FOI)	x						x
Holland	De Algemene Inlichtingen-en	x	x		x			x

Riik	Amet	Protseduurid						
		Kohtu luba	**Ministri luba**	**Prokuratuuri luba**	**Ameti juhi luba**	**Ametniku otsus**	**Juristi osalemine menetluses**	**Isiku teavitamine**
	Veiligheidsdienst (AIVD)							
	Militaire Inlichtingen-en Veiligheidsdienst (MIVD)	x	x		x			x
Saksamaa	Bundesamt für Verfassungsschutz (BfV)	x	x		x			x
	Der Militärischen Abschirmdienst (MAD)	x	x		x			x
	Bundesnachrichtendienst (BND)	x	x		x			x
UK	Security Service (MI5)		x		x			
	Secret Intelligence Service (MI6)		x		x			
	Government Communications Headquarters (GCHQ)		x		x			

11. LISA 3: JÄRELEVALVEMEHHANISMIDE VÕRDLEV TABEL

Riik	Amet	Järelevalve						
		Teenistuslik järelevalve	Prokuratuuri järelevalve	Parlamentaarne komisjoni	Õiguskantsler/ ombudsman	Spetsialiseerunud asutused/ institutsioonid	Spetsialiseerunud kohus	Andmekaitse inspektsioon
Eesti	Kaitsepolitseiamet	x	x	x	x			
	Teabeamet	x		x	x			
	Kaitsevägi	x		x	x			
Soome	Suojelupoliisi (SUPO)	x		x	x			
	Pääesikunnan Tiedusteluosasto (PVTK)	x		x	x			
Rootsi	Säkerhetspolisen (SÄPO)			x	x	x		x
	Försvarsmakten			x	x			x
	Försvarets Radioanstalt (FRA)			x	x	x		x
	Försvarets materielverk (FMV)			x	x			x
	Totalförsvarets forskningsinstitut, (FOI)			x	x			x
Holland	De Algemene Inlichtingen-en Veiligheidsdienst (AIVD)	x		x	x			

Riik	Amet	Järelevalve						
		Teenistuslik järelevalve	Prokuratuuri järelevalve	Parlamentaarne komisjoni	Õiguskantsler/ ombudsman	Spetsialiseerunud asutused/ institutsioonid	Spetsialiseerunud kohus	Andmekaitse inspektsioon
	Militaire Inlichtingen- en Veiligheidsdienst (MIVD)	x		x	x			
Saksamaa	Bundesamt für Verfassungsschutz (BfV)			x				x
	Der Militärischen Abschirmdienst (MAD)			x				x
	Bundesnachrichtendienst (BND)			x				x
UK	Security Service (MI5)	x		x		x	x	
	Secret Intelligence Service (MI6)	x		x		x	x	
	Government Communications Headquarters (GCHQ)	x		x		x	x	