Elektroonilise side seaduse ja sellega seonduvalt teiste seaduste muutmise eelnõu väljatöötamiskavatsus (sideandmete säilitamine ja kasutamine)

I. Probleem, sihtrühm ja eesmärk

1. Probleemi kirjeldus ja selle tekke põhjus

Riigikogu võttis 15.11.2007 vastu elektroonilise side seaduse muudatused, millega võeti Eesti õigusesse üle Euroopa Liidu direktiiv sideandmete säilitamise kohta[1]. Muudatused jõustusid 17.12.2007 ning nende kohaselt pidid sideettevõtjad säilitama teatud liiki sideandmeid mobiilside ning Internetiühenduste kasutamise kohta 1 aasta jooksul ning edastama neid andmeid seaduses sätestatud juhtudel ja eesmärkidel pädevatele asutustele (jälitus- või julgeolekuasutus, Finantsinspektsioon ja kohus). Hilisemate muudatustega elektroonilise side seaduses ja teistes seadustes andmete kasutamise eesmärke laiendati ning nähti ette juurdepääs ka mitmetele teistele asutustele kriminaalmenetluse, väärteomenetluse ning riikliku järelevalve teostamise eesmärkidel.

08.04.2014 tunnistas Euroopa Liidu Kohus oma *Digital Rights Ireland* kohtuotsusega C-293/12 ja C-594/12 eelpool nimetatud sideandmete säilitamise direktiivi kehtetuks. Ühtlasi leidis EL Kohus kohtuotsuses *Tele2 Sverige* seisukohale, et kuivõrd e-privaatsuse direktiiv on suunatud sideteenuse pakkujate õiguste ja kohustuste ühtlustamisele, hõlmab direktiiv ka selliseid seadusandlikke meetmeid, mida liikmesriik võta vastu e-privaatsuse direktiivi alusel, isegi kui selliste meetmete eesmärk on kuritegevuse vastane võitlus.

21.12.2016 läks Euroopa Liidu Kohus oma otsusega *Tele2 Sverige* kohtuasjas C-203/15 ja C-698/15 sideandmete säilitamise ja kasutamise küsimuses veelgi kaugemale ning leidis, et kehtiv nn e-privaatsuse direktiiv[2] ei võimalda senisel kujul andmete säilitamist.

[1] Euroopa Parlamendi ja nõukogu direktiiv 2006/24/EÜ, mis käsitleb üldkasutatavate elektrooniliste sideteenuste või üldkasutatavate sidevõrkude pakkujate tegevusega kaasnevate või nende töödeldud andmete säilitamist ja millega muudetakse direktiivi 2002/58/EÜ

[2] Euroopa Parlamendi ja nõukogu direktiiv 2002/58/EÜ, 12. juuli 2002, milles käsitletakse isikuandmete töötlemist ja eraelu puutumatuse kaitset elektroonilise side sektoris (eraelu puutumatust ja elektroonilist sidet käsitlev direktiiv)

Sideandmetena käsitletakse kõige üldisemalt liiklus- või asukohaandmed ja nendega seotud teavet, mis on vajalik abonendi või kasutaja kindlakstegemiseks.[3] Sideandmete säilitamisega seonduv regulatsioon on puutumises mitmete erinevate õigusaktidega. Põhiregulatsioon paikneb elektroonilise side seaduses (edaspidi ESS), kuid valdkond on veel tihedas seoses menetlusseadustike ning isikuandmete kaitse üldregulatsiooniga. Sideandmete säilitamise regulatsioon ei käsitle reaalajas toimuvat andmetöötlust (nt hädaabinumbrile helistaja positsioneerimine, abivajaja asukoha tuvastamine ilma hädaabikõneta jt) ega jälitustegevuse raames teostatavaid toiminguid. Sideandmete säilitamise reeglid ei puuduta sõnumi sisu, vaid üksnes sideseansiga seotud metaandmeid.

Sideandmete säilitamisel on mitu erinevat eesmärki. Ühest küljest säilitavad ettevõtjad andmeid kliendiga seotud lepingute täitmiseks ja arveldamiseks aga ka võrguliikluse statistika analüüsiks, pakkumiste vms tegemiseks. Kuigi neid andmeid kogutakse sõltumata riigi vajadustest, ei pruugita neid säilitada pikema ajaperioodi jooksul. Teisest küljest on leitud, et kuna andmete säilitamine on osutunud nii vajalikuks ja tõhusaks õiguskaitsevahendiks mitmes liikmesriigis toimunud uurimiste käigus, eriti selliste raskete juhtumite puhul nagu organiseeritud kuritegevus ja terrorism, on vaja tagada säilitatud andmete kättesaadavus õiguskaitseasutustele teatava ajavahemiku jooksul. Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikli 8 nõuetele vastava andmete säilitamise vahendi vastuvõtmine on seetõttu vajalik meede.[4] Sideandmete säilitamine on täpsemalt vajalik süütegude avastamiseks, ennetamiseks, tõkestamiseks ja kohtus menetlemiseks. Samuti võivad sideandmed olla vajalikud muude menetluste raames vajaliku tõendusteabe saamiseks, sh tsiviilkohtumenetluses, erinevates loamenetlustes ning riikliku julgeoleku tagamise eesmärkidel. Sideandmete kasutamine on oluline ka mitme teise tegevuse puhul, sealhulgas mitmed korrakaitselised tegevused (nt hädaabi numbri pahatahtliku kasutamine takistamine).

Seega on sideandmete säilitamisel mitu erinevat väljundit, mis omakorda mõjutavad andmete kasutamise lubatavust ja proportsionaalsust. Ühest küljest tuleb analüüsida andmete säilitamist ning teisest küljest nende edasisi kasutamise eesmärke ning nende eesmärkide proportsionaalsust.

Väljatöötamiskavatsuse eesmärgiks on leida lahendused järgmistele probleemidele.

Sideandmete säilitamine

Euroopa Liidu Kohus on oma otsustes öelnud, et senine liikmesriikide praktika, mis tugines varasemale sideandmete säilitamise direktiivile ning mis seisnes sideandmete ühetaolises säilitamises valimatult kõikide isikute, kõikide sideseansside ja kõikide sidevahendite kohta ei ole kooskõlas Euroopa Liidu põhiõiguste hartaga, ei ole proportsionaalne ning riivab liigselt andmesubjektide õigusi. Kohtuotsused (eeskätt *Tele2 Sverige)* puudutasid sideandmete säilitamist kriminaalmenetluse eesmärkidel, seega hetkel puudub veel ühtne vastus küsimusele, kas EL õigusest tulenevad nõuded tuleb rakendada ka andmete säilitamisel riikliku julgeoleku tagamise eesmärkidel (pooleli olev kohtuasi C-623/17).

Sellest tulenevalt ei saa enam Eesti kehtivat õigust, mis kohustab sideettevõtjaid säilitama sideandmeid kõikide isikute kohta, kõikide sideseansside ja kõikide sidevahendite, muuta.

Sideandmete kasutamine

[3] Andmete säilitamise direktiivi art 2 lõige 2 punkt 1.
[4] Andmete säilitamise direktiivi pp 9.

Euroopa Liidu kohus leidis, et sideandmete kasutamine peab olema piiritletud ning lubatud raskete kuritegude avastamise ning uurimise eesmärgil. Vajalik on ette näha tõhus kontroll sideandmete päringute tegemise ning sideandmete kasutamise üle.

Kehtivas õiguses sätestatud piirid, millal sideandmete kasutamine on lubatud, on laiad, jättes seeläbi pädevatele asutustele liialt laia diskretsiooni. Piisavaks on peetud vältimatu vajalikkuse kriteeriumi sätestamist, jättes nõude sisustamise igakordseks kaalutlusotsuseks. Näiteks sätestab KrMS § 90[1] lg 3 sõnaselgelt *ultima ratio* põhimõtte ning lubab teha päringu sideettevõtjale üksnes siis, kui see on vältimatult vajalik kriminaalmenetluse eesmärgi saavutamiseks. See ei pruugi siiski olla piisav, tagamaks kooskõla Euroopa Kohtu praktikaga. Liialt lai diskretsioon võib luua eeldusi olukordadeks, kus sideandmete kasutamine ei ole proportsionaalne ning andmesubjektide õiguste riive ulatuslikum kui lubatud. Kohus on leidnud, et vajalik on ette näha täpsemad tingimused ning üksnes vajalikkuse ja proportsionaalsuse põhimõttest lähtumine ei pruugi olla piisav.

Andmekaitsenõuete järgimine

Isikuandmete kaitse seadusest (edaspidi IKS) tulenevalt kohalduvad seadusest tulenevad reeglid, k.a. sõltumatu järelevalve teostamise regulatsioon, ka kriminaalmenetlusele ja kohtumenetlusele menetlusseadustikes sätestatud eranditega. Üldreeglina teostab isikuandmete töötlemise üle sõltumatut järelevalvet Andmekaitse Inspektsioon. Arvestades, et menetlusseadustikes ei ole sätestatud sideandmete kasutamise üle järelevalve teostamist, võib tekkida vastuolu Euroopa Kohtu praktikast tuleneva sõltumatu järelevalve nõudega, kuivõrd ei ole selge, kas ja millistel juhtudel on Andmekaitse Inspektsioonil võimalik teostada järelevalvet sideandmete kasutamise üle. Tõhusa ja sõltumatu järelevalve nõue tuleneb ka mais 2018.a jõustunud EL andmekaitsereformi õigusaktidest (andmekaitsedirektiivist[5] ja uuest andmekaitse üldmäärusest[6]).

Kuigi üldreeglina kohalduvad IKS-ist tulenevad reeglid ka kriminaalmenetlusele ja kohtumenetlusele, ei ole kõigi andmesubjekti õiguste rakendamine erinevates menetlustes võimalik. Arvestades, et õigus isikuandmete kaitsele on igaühe põhiõigus ning andmesubjekti õigused tema kohta käivate andmete töötlemisel on isikuandmete kaitse üks peamisi väljundeid, tuleb seadusandjal luua andmesubjekti jaoks tõhusad mehhanismid, mille kaudu neid õigusi teostada. Üks olulisemaid elemente on seejuures isiku õigus olla tema kohta käivate andmete töötlemisest teavitatud.

2. Sihtrühm

Andmete säilitamise ja kasutamise osas on sihtrühmaks esmalt uurimisasutused, prokuratuur, kohus, julgeolekuasutused ning teised valitsusasutused, kes kasutavad sideandmeid erinevat liiki menetlustes. Teiseks kuuluvad sihtrühma sideettevõtjad, kellel lasub kohustus sideandmeid säilitada ning võimaldada pädevate asutuste juurdepääs nendele andmetele. Kolmandaks kuuluvad sihtrühma kõik isikud, kes kasutavad Eestis sideteenuseid (mobiiltelefoniside, -andmeside ja Internet) ning kellega seotud sideandmeid säilitatakse ja kasutatakse.

---

[5] Euroopa Parlamendi ja nõukogu direktiiv (EL) 2016/680, 27.aprill 2016, mis käsitleb füüsiliste isikute kaitset seoses pädevates asutustes isikuandmete töötlemisega süütegude tõkestamise, uurimise, avastamise ja nende eest vastutusele võtmise või kriminaalkaristuste täitmisele pööramise eesmärgil ning selliste andmete vaba liikumist ning millega tunnistatakse kehtetuks nõukogu raamotsus 2008/977/JSK

[6] Euroopa Parlamendi ja nõukogu määrus (EL) 2016/679, 27.aprill 2016, füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus)

3. Eesmärk ja saavutatava olukorra kirjeldus

Väljatöötamiskavatsuses kirjeldatud probleemide lahenduste elluviimise eesmärgid on alljärgnevad.

Regulatsiooni muutmise eesmärk on sätestada senisest täpsemad ja selgemad kriteeriumid olukordadele, millal on lubatud sideandmeid säilitada ning hiljem neid eri liiki menetlustes kasutada, tagades seeläbi isiku eraelu puutumatuse ja isikuandmete parema kaitse. Justiitsministeeriumi hinnangul on sideandmete kasutamine eri liiki menetlustes tõendusteabe hankimisel hädavajalik, kuid seejuures tuleb kõrgel tasemel tagada isikuandmete kaitse ning andmesubjektide õigused. Arvestades uuenenud kohtupraktikat on vajalik viia kehtiv õigus kohtu poolt täpsustatud tõlgendustega kooskõlla. Hetkel toimiva ning kõiki kasutajaid hõlmava üldise säilitamise kohustuse asemel tuleb näha ette sideandmete piiritletud säilitamine ja kasutamine.

Eesmärk on seaduste muutmisega saavutada olukord, kus sideandmete säilitamine ning kasutamine on selgelt ja detailselt reguleeritud ning vastab Euroopa Liidu Kohtu praktikale. Tulevane regulatsioon lähtuks proportsionaalsuse põhimõttest ning näeks ette senisest kitsamad ning täpsemad kriteeriumid sideandmete kasutamiseks, muudaks selgemaks reeglid sideandmete päringute tegemise ning päringute ning andmete kasutamise järelevalve üle, reguleeriks täpsemalt ühes menetluses kogutud sideandmete kasutamise teistes menetlustes ning seeläbi näeks ette selgelt ja andmesubjektidele arusaadavalt nende õigused nende kohta käivate andmete töötlemise üle. Hetkel on sideandmete kasutamine võimalik paljude erinevate menetluste puhul ning juurdepääs sideandmetele on samuti mitmetel asutustel. Lähtuvalt Euroopa Kohtu praktikast tuleb andmete kasutamise reeglid üle vaadata, andmetele juurdepääsu tingimused täpsustada ja andmete kasutamise alused piirata. Arvestades Euroopa Kohtu poolt antud hinnanguid tuleb seaduse tasandil sätestada olukorrad, millal on andmete kasutamise võimalus proportsionaalne.

II. Hetkeolukord, uuringud ja analüüsid

4. Kehtiv regulatsioon, seotud strateegiad ja arengukavad

Sideandmete säilitamise kohustus on reguleeritud ESS §-s 111[1], kuid andmetele juurdepääsu reguleeritakse nii vastava sätte lõikes 11, ESS §-s 112 ning §-s 114[1] kui ka menetlusseadustikes (KrMS § 90[1], VTMS § 31[2], TsMS tõendite hankimise alused ja reeglid, sh TsMS § 278jj) ja muudes erivaldkonna seadustes. Andmete säilitamise kohustus sätestati ESS-s 2007. a lõpus ning alus oli 15.03.2006 vastuvõetud Euroopa Parlamendi ja nõukogu direktiiv 2006/24/EÜ, mis käsitleb üldkasutatavate elektrooniliste sideteenuste või üldkasutatavate sidevõrkude pakkujate tegevusega kaasnevate või nende töödeldud andmete säilitamist ja millega muudetakse direktiivi 2002/58/EÜ (edaspidi andmete säilitamise direktiiv).[7]

Euroopa Kohus tunnistas oma 8.04.2014.a otsusega kohtuasjades C-293/12 ja C-594/12 (edaspidi andmete säilitamise kohtuotsus) ülalmainitud direktiivi kehtetuks. Kohtu hinnangul ei olnud kokkuvõttes tegemist proportsionaalse regulatsiooniga. Andmete säilitamise direktiiv on küll kehtetuks tunnistatud, mistõttu seal sisalduvaid põhimõtteid ei pea liikmesriigid enam

[7] Euroopa Kohus tunnistas oma 08.04.2014 otsusega kohtuasjades C-293/12 ja C-594/12 direktiivi kehtetuks tulenevalt sellest, et kohtu hinnangul ei olnud kokkuvõttes tegemist proportsionaalse regulatsiooniga

järgima. Käesolevas analüüsis võetakse siiski aluseks ka Euroopa Kohtu kaalutlused direktiivi proportsionaalsuse hindamisel.

Andmed, mida sideettevõtja on kohustatud säilitama, on ammendavalt sätestatud ESS §-s 111^1 lõigetes 2 ja 3 ning nende andmete säilitamisega seonduvad toimingud ESS §-s 111^1 lg-s 1. Nimetatud regulatsioon vastas andmete säilitamise direktiivi artiklile 5. Eelnimetatud andmete säilitamine peab tagama sideallika seiramise ja tuvastamise, side sihtpunkti tuvastamise, side kuupäeva, kellaaja ja kestuse kindlaksmääramise, sideteenuse liigi kindlaksmääramise, sideteenuse kasutaja terminalseadme või oletatava terminalseadme kindlaksmääramise ning terminalseadme asukoha kindlaksmääramise.

ESS loob õigusliku aluse, mis võimaldab sideettevõtjatel kalduda kõrvale rangetest konfidentsiaalsuse nõuetest, isikuandmete kaitse põhimõtetest ning väljastada andmeid andmesubjekti nõusolekuta kolmandatele isikutele.
Üldreeglina tohivad isikuandmete töötlejad säilitada üksnes sellised andmed, mis on vajalikud lepingust tulenevate kohustuste täitmiseks, ning üksnes lepingu täitmiseks vajaliku perioodi jooksul. Sideandmete säilitamise ja kasutamise reeglid on seega erand.
Sideettevõtjatele kohalduvad reeglid isikuandmete kaitse valdkonnas tulenevad eeskätt e-privaatsuse direktiivist, mis on Eestis üle võetud eelkõige ESS-i normidega. Samuti kehtib sideettevõtjate osas IKS ning EL andmekaitsereeglistik.
Kehtiv ESS näeb ette sideettevõtjate kohustuse väljastada teatud sideandmed pädevatele asutustele ning loetleb asutused, kellele sideettevõtjad peavad andmed edastama (ESS § 111^1 lg 11). Iga konkreetse menetlusliigi kohta käivad regulatsioonid paiknevad omakorda eriseadustes, kus on ühtlasi sätestatud ka andmetele juurdepääsu tingimused, juurdepääsuks lubade andmine ning andmete kasutamise eesmärgid. Teatud juhtudel väljastatakse andmed üksikpäringuna, st seoses konkreetse sideseansiga.

Kehtiva korra alusel on sideandmetele juurdepääs olemas:
- uurimisasutustel, jälitusasutustel, prokuratuuril ja kohtul kriminaalmenetluses vajaliku teabe kogumiseks;
- julgeolekuasutustel põhiseadusliku korra kaitse eesmärgil;
- Andmekaitse Inspektsioonil, Finantsinspektsioonil, Keskkonnainspektsioonil, Politsei- ja Piirivalveametil, Kaitsepolitseiametil ning Maksu- ja Tolliametil väärteomenetluses vajaliku teabe kogumiseks;
- Finantsinspektsioonil väärtpaberituru seaduses sätestatud juhtudel riikliku järelevalve teostamise eesmärgil;
- kohtul tsiviilvaidluste lahendamise eesmärgil;
- jälitusasutustel kriminaalmenetluse väliste toimingute tegemiseks isiku suhtes, kelle puhul on põhjendatult alust arvata, et ta paneb toime kuriteo või isiku suhtes, kes on kuulutatud tagaotsitavaks;
- pädevatel asutustel tausta- ja julgeolekukontrolli teostamise eesmärgil.

Kehtiva õiguse järgi säilitavad sideettevõtjad sideandmeid üldjuhul 1 aasta jooksul alates andmete loomisest sideteenuse osutamise käigus või andmete töötlemisest. Sideandmete päringute tegemisel eristatakse kahte liiki päringuid:
- nn omanikupäringud, mille raames edastatakse pädevale asutusele üksnes konkreetse teenuse kasutaja kliendiandmed;
- muude andmete päringud, mis võimaldavad tuvastada kliendi suhtluspartnereid, liikumistrajektoori jt.

Andmete saamiseks päringu esitamise võimalus on reguleeritud osaliselt ESS-s, osaliselt menetlusseadustikes (KrMS, VTMS), aga ka korrakaitseseaduse §-s 35 ning terves hulgas

eriseadustes (nt politsei- ja piirivalveseadus, tolliseadus, maksukorralduse seadus, julgeolekuasutuste seadus jt). Normide omavaheline koosmõju on ebaselge, samamoodi on väga erinev ning ebaühtlane normide täpsus, ulatus ja rakendusala. Sellest tulenevalt on valdkond väga ebaühtlaselt reguleeritud ning puudub selge ülevaade selle kohta, kes, kui palju ja milliseid päringuid millistel alustel teostab.

Omanikupäringute puhul on isiku põhiõiguste riive ulatus väiksem ning seega on ka sellistele päringutele ette nähtud reeglid leebemad, kui muude andmete päringute esitamisel. Päringute tegemise reeglid on eri liiki menetlustes mõneti erinevad, samuti on erinevad andmesubjektide õiguste ulatus ning muud asjakohased nõuded. Päringu alusel saadud sideandmete edasisele töötlemisele ja säilitamisele kohalduvad eriseadustest tulenevad reeglid.
Järelepärimiste osas peetakse üldist statistikat, mis hõlmab mh järelepärimiste arvu, mille korral teave edastati ning järelepärimiste arvu, mille kohta ei olnud võimalik teavet edastada.

Kuigi EL Kohtu otsused *Digital Rights Ireland* ja *Tele2 Sverige* ei toonud automaatselt kaasa Eesti õiguse kehtetuse, mõjutavad kohtuotsused siiski märkimisväärselt ka Eesti õiguskorda. Kuigi pärast andmete säilitamise direktiivi kehtetuks tunnistamist on EL liikmesriikidel justkui võimalik endil otsustada sideandmete säilitamisele kohaldatavad reeglid, tulenevad täiendavad piirangud lisaks Eesti riigisisestele normidele (sh põhiseadus) ka rahvusvahelistest õigusaktidest. Kuigi *Tele2 Sverige* kohtuotsus möönab, et sideandmete säilitamine ja kasutamine on vajalik kuritegevuse vastu võitlemiseks, leitakse siiski, et senine ühetaoline sideandmete säilitamine isikute ja geograafiliste piirkondade lõikes ei ole kooskõlas EL põhiõiguste harta ning e-privaatsuse direktiivi artikli 15 lõikega 1[8]. Sideteenuse osutamise, aga ka isikuandmete kaitse valdkonnad on EL-is ühtlustatud ning liikmesriikide võimalus sätestada sideettevõtjate konfidentsiaalsuskohustusest erandi tuleneb e-privaatsuse direktiivist.
Andmete säilitamise regulatsiooni juures tasub tähele panna mitut olulist küsimust, mida tuleb arvestada edasise põhiseaduslikkuse analüüsi koostamisel. Esiteks – ESS regulatsiooni kohaldamisala ja eesmärgid on oluliselt laiemad kui algse ülevõetava direktiivi eesmärk. Nimelt oli andmete säilitamise direktiivi normistik suunatud raskete ning organiseeritud kuritegude vastu võitlemisele. ESS-s on aga näiteks väärteomenetluses vastava teabe kasutamine, mis ei lähtu eesmärgist, et andmeid kasutataks ainult raskete kuritegude menetlemiseks. Samuti on sätestatud andmete väljastamine tsiviilvaidluste lahendamiseks (piiritlemata eesmärgil), mida ülalmainitud direktiiv ei käsitle.

Teiseks tuleb meeles pidada Euroopa Liidu õiguse kohaldamisala. ESS ja mõned eriseadused viitavad valdkondadele, mille osas ei ole Euroopa Liidul pädevust võtta seadusandlikke meetmeid. Näiteks julgeoleku ja riigikaitse valdkonnale andmete säilitamise direktiivi laiendamine tervikuna on selles valguses küsitav.

Kolmandaks tuleb tähele panna, et andmete säilitamise regulatsioon kohaldub nii füüsilistele kui ka juriidilistele isikutele. See tähendab, et sideandmete päringuid võidakse teha nii juriidiliste kui ka füüsiliste isikute kohta. Samas ei kaitse isikuandmete kaitse sätted juriidilisi isikuid. Eeldatakse, et juriidilistel isikutel ei ole isikuandmeid. Kuna iga juriidilise isiku taga

[8] Liikmesriigid võivad võtta seadusandlikke meetmeid, millega piiratakse käesoleva direktiivi artiklites 5 ja 6, artikli 8 lõigetes 1, 2, 3 ja 4 ning artiklis 9 sätestatud õiguste ja kohustuste ulatust, kui selline piiramine on vajalik, otstarbekas ja proportsionaalne abinõu selleks, et kaitsta direktiivi 95/46/EÜ artikli 13 lõikes 1 nimetatud riiklikku julgeolekut (s.t riigi julgeolekut), riigikaitset, avalikku korda, kriminaalkuritegude või elektroonilise sidesüsteemi volitamata kasutamise ennetamist, uurimist, avastamist ja kohtus menetlemist. Selleks võivad liikmesriigid muu hulgas võtta seadusandlikke meetmeid, millega nähakse ette andmete säilitamine piiratud aja jooksul käesolevas lõikes sätestatud põhjustel. Kõik käesolevas lõikes osutatud meetmed on kooskõlas ühenduse õiguse üldpõhimõtetega, kaasa arvatud Euroopa Liidu lepingu artikli 6 lõigetes 1 ja 2 osutatud põhimõtetega.

on siiski füüsilised isikud, tuleb põhiseaduslikkuse kontekstis analüüsida, milliseid ja kas ka erinevaid garantiisid, on vajalik pakkuda juriidiliste ja füüsiliste isikute lõikes.

Viimaseks tuleb mõelda, kas erisused esinevad isikustatud ja isikustamata[9] sideandmete töötlemise vahel. Isikustamata andmetele ei laiene isikuandmete kaitse õigus. Seetõttu ei laine neile näiteks põhiseadusest tulenevad tagatised eraelu puutumatuse osas. kuna sideandmete päringu eesmärk on peamiselt kellegi tuvastamine, mitte anonüümsete andmete uurimine, siis võib isikustamata andmete kombineerimisel teiste andmetega andmesubjekti isik välja tulla. Siis on tegu isikustatud andmetega ja tuleb kohaldada vastavat regulatsiooni.

Käesoleval ajal on EL Kohtus menetluses veel kaks sideandmete säilitamist puudutavat eelotsusemenetlust. Kohtuasjas C-207/16 (Hispaania) soovitakse EL Kohtu hinnangut selle kohta, milliseid kuritegusid saab senise EL Kohtu praktika valguses käsitleda raskete kuritegudena, mille puhul oleks säilitatud sideandmete kasutamine proportsionaalne. Otsust võib loodetavasti oodata 2018.a jooksul, suuline istung toimus 29.01.2018. 3.mail 2018.a esitas EL Kohtu kohtujurist oma arvamuse kohtuasjas C-207/16[10], mille kohaselt tuleks e-privaatsuse direktiivi tõlgendada selliselt, et sideandmete päring sellise kuriteo menetluse raames, kus toimus röövimine ning isikule (raske) tervisekahjustuse tekitamine, on proportsionaalne ega ole seetõttu EL õigusega vastuolus. Kohtujurist leidis, et pole tingimata vaja, et kuriteod, mis konkreetses kohtuasjas kasutatud piiravat meedet (sideandmete kasutamist) õigustavad, peaksid olema käsitatavad „rasketena“ kohtuotsustest *Digital Rights* ja *Tele2* tuleneva kohtupraktika tähenduses. Kuritegu, millega riivet õigustatakse, peab eriti raske olema vaid juhul, kui riive ise on eriti raske. Kui riive ei ole raske, saab seda õigustada mis tahes liiki „kriminaalkuriteoga“. Seega leidis kohtujurist, et direktiivi 2002/58 artikli 15 lõiget 1 koosmõjus harta artiklitega 7 ja 8 ning artikli 52 lõikega 1 tuleb tõlgendada nii, et meetmega, mis võimaldab liikmesriigi pädevatel asutustel saada kuritegude vastase võitluse eesmärgil juurdepääs konkreetses mobiiltelefonis piiratud ajavahemiku jooksul aktiveeritud telefoninumbrite kasutajate isikusamasuse tuvastamist võimaldavatele andmetele, kaasneb direktiivi ja hartaga tagatud põhiõiguste riive, mis ei ole piisavalt raske selleks, et selline juurdepääs peaks piirduma üksnes olukordadega, kus tegemist on raske kuriteoga. Lisaks arvas kohtujurist, et mõiste „raske kuritegu“ kohtuotsustest Digital Rights ja Tele2 tuleneva Euroopa Kohtu praktika tähenduses ei kujuta endast liidu õiguse autonoomset mõistet, mille sisu peaks kindlaks määrama Euroopa Kohus. Liikmesriigid peavad aga siiski direktiivi 2002/58 artikli 15 lõikest 1 tulenevat erandit rakendama kooskõlas liidu õigusest tulenevate kohustustega, eriti hartaga tagatud põhiõigustega, ning see allub Euroopa Kohtu kontrollile. Teise võimalusena, kui kohus asub seisukohale, et mõiste „raske kuritegu“ on käsitatav liidu õiguse autonoomse mõistena, tuleb kuriteo raskust, mis õigustab liikmesriigi pädevate asutuste juurdepääsu andmetele, *mõõta mitte ainult ettenähtud karistusest lähtudes, vaid võttes arvesse lisaks ka kõiki teisi objektiivseid hindamiskriteeriume.* Ning kolmanda võimalusena, kui selleks, et kvalifitseerida kuritegu senise kohtupraktika tähenduses „raskena“, tuleb arvesse võtta üksnes selle eest ette nähtud karistust, võivad liikmesriigid selleks kohase minimaalse karistuse ise kindlaks määrata, kui nad teevad seda kooskõlas liidu õigusest tulenevate nõuetega, eeskätt nõudega, et harta artiklites 7 ja 8 tagatud põhiõiguste riive peab jääma erandlikuks ja olema kooskõlas proportsionaalsuse põhimõttega.

Eelotsusemenetluses C-623/17 (Ühendkuningriik) soovitakse saada vastust, kas EL kohtupraktikat tuleb teatud ulatuses kohaldada ka sideandmete säilitamisele ja kasutamisele rahvusliku julgeoleku (*national security)* eesmärkidel, kuigi julgeolekuvaldkond ise jääb EL

[9] Isikustamata andmed – andmed, mille kaudu ei ole võimalik füüsilist isikut tuvastada.
[10] Kohtujuristi ettepanek:
http://curia.europa.eu/juris/document/document.jsf?text=&docid=201707&pageIndex=0&doclang=ET&mode=lst&dir=&occ=first&part=1&cid=425870

õiguse kohaldamisalast välja. Liikmesriigid esitasid oma seisukohad veebruaris 2018, EL Kohtult ei ole hetkel veel saabunud täiendavaid küsimusi suulisel istungil käsitlemiseks ega suulise istungi aega. Hetkel teadaolevalt võib istung aset leida 2018.a lõpus.

Juulis 2018 esitas Belgia kohus samuti eelotsuse taotluse EL Kohtule seoses e-privaatsuse direktiivi artikli 15 lg 1 tõlgendusega. Kohtuasja number on C-520/18. Augustis 2018 esitas eelotsuse taotluse ka Prantsusmaa, kohtuasja number on C-511/18. Kohtuasi C-511/18 on seotud põhiõiguste riive proportsionaalsuse hindamisega riigi julgeoleku eesmärgil teostatavate toimingute raames. Esialgselt on Eesti otsustanud sekkuda mõlemasse menetlusse.

Eesti riigisiseste õigusnormide aluseks on eeskätt e-privaatsuse direktiivi art 15 lg 1. Sisuliselt teostab Eesti seadusandja ESS-i ja eriseaduste kaudu oma e-privaatsuse direktiivist tulenevat õigust kehtestada riigisisene sideandmete säilitamise raamistik, kui see on vajalik art 15 lõikes 1 toodud eesmärkide saavutamiseks. Sellisteks eesmärkideks on:

- riigi julgeoleku tagamine;
- riigikaitse;
- avalik julgeolek (avaliku korra kaitse, *public security)*
- süütegude avastamine, ennetamine, uurimine ja nende eest süüdistuse esitamine (kuritegude menetlemine).

Alates 2017.a on EL-is menetluses uue e-privaatsuse määruse eelnõu, millega asendatakse hetkel kehti e-privaatsuse direktiiv. Määruse eelnõu arutelude käigus on korduvalt arutatud ka võimalikke lahendusi seoses sideandmete säilitamisega. Liikmesriigid ei soovi reguleerida sideandmete säilitamist e-privaatsuse määruses, kuid kindlasti peab säilima võimalus teha määruses sätestatud rangetest reeglitest erandid, mille alusel oleks võimalik kas EL või riigisisese õigusega näha ette sideandmete säilitamise ja edasise kasutamise reeglid õiguskaitse eesmärkidel. Selline lähenemine on kooskõlas ka EL Kohtu praktikaga, kes küll tühistas sideandmete säilitamise direktiivi ning kehtestas teatud tingimused sellele, mida peaks andmete säilitamise ja kasutamise reguleerimisel arvestama, kuid ei keelanud andmete säilitamist kui sellist. Kohus rõhutas vajadust pidada kinni EL põhiõiguste hartast tulenevatest põhimõtetest ja nõuetest, tagades seeläbi sideandmete säilitamise raamistiku kooskõla EL õigusega. Seda kinnitab hetkel ka kohtujuristi arvamus kohtuasjas C-207/16.

Kehtivatest siseriiklikest strateegilistest dokumentidest on kõnelause temaatikaga seotud ennekõike Vabariigi Valitsuse tegevusprogramm, on terrorismivastase võitluse tõhustamine üks Siseturvalisuse arengukava eesmärke. Vabariigi Valitsuse 29.05.2015 korraldusega nr 231 kinnitatud „Vabariigi Valitsuse tegevusprogramm 2015-2019“ punkt 12.22 "Julgeolekuolukorra muutusest tulenevalt tõstame Teabeameti ja kaitseväe luure- ja KAPO vastuluurevõimekust ning Keskkriminaalpolitsei võimekust raske kuritegevuse tõkestamisega tegelemisel", mille raames on eraldi välja toodud elektroonilise side seaduse muutmise vajadus. Vabariigi Valitsuse tegevusprogramm punkt 11.16 "Muudame õigusrikkumiste menetlemise (sh kriminaalmenetluse) paindlikumaks ja lihtsamaks, tagades menetluse inimest vähimal koormaval viisil ning arvestades rikkumiste raskusastet ja tagajärgi. Selleks uuendame kriminaalmenetluse seadustikku. Kriminaalmenetluse kiirendamiseks tõhustame politsei ja prokuratuuri töökorraldust."

5. Tehtud uuringud

Väljatöötamiskavatsuse aluseks on Justiitsministeeriumis 2014.-2015.a jooksul läbi viidud valdkonna analüüs (avaldamata), analüüsitud on Euroopa Kohtu lahendeid ning läbi on viidud asjakohaste regulatsioonide kaardistamine.

Samuti on väljatöötamiskavatsuse koostamise juures arvestatud EL Nõukogu vastavas töörühmas (DAPIX – *Friends of Presidency Data Retention)* liikmesriikide ja EL ametiasutuste (Europol, Eurojust, Terrorismivastane koordinaator, Nõukogu õigusteenistus jt) arutatud lahendusettepanekuid ja soovitusi. Vastav töögrupp on kokku kutsutud just selleks, et arutada liikmesriikides pärast EL Kohtu otsuseid tekkinud olukorda seoses sideandmete säilitamise ja kasutamisega ning hinnata võimalikke lahendusi EL tasandil. Töögrupp kutsuti kokku 2017. aasta kevadel ning on siiani aktiivselt jätkanud EL liikmesriikides sideandmete säilitamise ja kasutamisega seotud arutelusid.

6. Kaasatud osapooled

Justiitsministeerium konsulteeris erinevate osapooltega, sealhulgas Majandus- ja Kommunikatsiooniministeeriumi ning Siseministeeriumiga ning Andmekaitse Inspektsiooniga.

Sideandmete säilitamise ja kasutamise küsimust on arutatud ka mitmel Justiitsministeeriumi poolt korraldatud ümarlaual, kus osalesid lisaks Justiitsministeeriumi esindajatele, Majandus- ja Kommunikatsiooniministeeriumi, Siseministeeriumi, Andmekaitse Inspektsiooni, Kaitsepolitseiameti, Politsei- ja Piirivalveameti, Riigiprokuratuuri ja Õiguskantsleri Kantselei esindajad. Justiitsministeerium ja Majandus- ja Kommunikatsiooniministeerium on konsulteerinud ka sideettevõtjatega ning huvigruppidega.

III. Probleemi võimalikud mitteregulatiivsed lahendused

7. Kaalutud võimalikud mitteregulatiivsed lahendused

Avalikkuse teavitamine	EI
Rahastuse suurendamine	EI
Mitte midagi tegemine ehk olemasoleva olukorra säilitamine	JAH
Senise regulatsiooni parem rakendamine	JAH

Justiitsministeeriumi hinnangul ei ole avalikkuse teavitamine ega rahastuse suurendamine käesoleva VTK sisu arvestades asjakohased, mistõttu neid lahendusi ei ole kaalutud. Sideandmete säilitamine ning kasutamine on ette nähtud seadusega, kuid muutunud kohtupraktika valguses on otsustada, kas Eesti soovib säilitada olemasolevat regulatsiooni või muuta kehtivat raamistikku lähtuvalt muutunud rahvusvahelisest õigusest ja praktikast. Väljatöötamiskavatsuse koostamise raames on kaalutud, kas olukorra lahendamine on võimalik ilma mistahes muudatusi tegemata või läbi kehtiva regulatsiooni parema rakendamise.

Väljatöötamiskavatsuse koostamisel on kaalutud olemasoleva olukorra säilitamise võimalikkust. Uuenenud kohtupraktika ning rahvusvahelise õiguse ja kehtiva Eesti õiguse omavahelise kooskõla arutamiseks on Justiitsministeeriumi alates 2014.a kohtunud erinevate asutuste ning huvigruppidega. Laiaulatuslike arutelude käigus on ilmnenud, et kehtiva olukorra säilitamine ei ole hetkel sobilik lahendus ning õigusraamistik tuleb muuta. Sellest tulenevalt on Justiitsministeeriumi hinnangul hetkel ilmne, et kehtiva olukorra säilitamine ei ole antud juhul võimalik ega asjakohane.

Vaatamata 2014.a ja 2016.a Euroopa Kohtu otsustele ning muutunud rahvusvahelisele õigusele, sh sideandmete direktiivi kehtetuks tunnistamisele on Eesti riigisisene sideandmete säilitamise regulatsioon jätkuvalt kehtiv. Olemasolev Eesti regulatsioon on vastu võetud nõuetekohase seadusandliku menetluse raames ning kuigi ESS § 111^1-114^1 võeti üle mh ka sideandmete säilitamise direktiiv, on tegemist Eesti õiguskorra kehtiva osaga. Riigikohus on oma

23.02.2015.a lahendis nr 3-1-1-51-14 hinnanud Eestis kuni 2013.a jaanuarini kehtinud sideandmete säilitamise regulatsiooni põhiseaduspärasust ning asunud seisukohale, et kehtestatud normid on põhiseaduspärased. Kriminaal- ja väärteomenetluses on sideandmete menetluses kasutamise tingimusena selgelt sätestatud *ultima ratio* põhimõtte kohaldamine, mis võimaldab pädevatel asutustel endil hinnata olukordi, millal on sideandmete kasutamine proportsionaalne. Üldreeglina kehtib vastav põhimõte ka laiemalt avaliku võimu sekkumisel üksikisiku eraellu. Siiski on põhiseaduse §-st 14 lähtuvalt seadusandja ülesanne tagada isikute põhiõigusi ja vabadusi, mistõttu peab seadusandja selgelt piiritlema ametiasutuste diskretsiooni ulatuse seaduse tasandil, kehtestades vajalikud kriteeriumid põhiseaduse §-st 11 tuleneva proportsionaalsuse nõude hindamiseks. Liialt ulatusliku diskretsiooni sätestamine võib viia normide laia tõlgendamiseni ning selle tõttu üksikisikute õiguste ebaproportsionaalse riiveni.

Arvestades *ultima ratio* põhimõtte olemasolu riigisiseses õiguses, oleks võimalik anda pädevatele asutustele juhiseid ja selgitusi põhimõtte parema rakendamise jaoks, selgitades kaalutlusõiguse ulatuse piirid. Samuti on tõlgendamise teel ning läbi praktika kujundamise võimalik osaliselt lahendada ka järelevalve- ning loamenetlusega seonduvad probleemid. Siiski tuleb arvestada, et regulatsioon riivab ulatuslikult isiku põhiõigusi, mistõttu ei anna kehtiva õiguse parem selgitamine ja tõhusam rakendamine soovitud tulemust. Samuti on kehtiv regulatsioon küllaltki killustatud ning ebaselge, mistõttu ka normide parem rakendamine võib olla raskendatud. Praegusel hetkel on ilmne, et kuigi sideandmete regulatsiooni parem rakendamine ning senisest rangem lähenemine andmete kasutamisele on möödapääsmatult vajalikud, ei ole kehtiva õiguse raames võimalik kindlustada kooskõla uuendatud EL õigusega ning kohtupraktikaga. Seetõttu tuleb õigusnormide paremat rakendamist rakendada koosmõjus regulatiivsete muudatustega, kindlustades seeläbi praktikute parema arusaama sideandmete säilitamise ja kasutamisega seotud probleemidest ning tagades uuendatud õiguskorra parem ja tõhusam rakendamine. Sellest tulenevalt tuleb Justiitsministeeriumi hinnangul kõigepealt muuta kehtivat õigust, tõstes seejuures õigusnormide rakendajate teadlikkust sideandmete regulatsiooniga kaasnevatest riskidest isikute põhiõigustele. Kuna nõudmised sideandmete säilitamisele ja kasutamisele on muutunud kõrgemaks, ei ole käesoleval juhul võimalik olemasoleva olukorra säilitamine või olemasoleva regulatsiooni parem rakendamine. Eesti õigus praegusel hetkel ei vasta täielikult Euroopa Kohtu otsustes toodud nõudmistele ning vajalik on regulatsiooni muutmine.

Arvestades kehtivate normidega seonduvate probleemide ulatust ning muutunud kohtupraktikat on kehtiva regulatsiooni muutmine optimaalne lahendus. Uue regulatsiooniga oleks võimalik lahendada erinevad tõusetunud probleemid ning näha ette võimalikult ühtsed reeglid eri liiki menetlustes, tõhustades seeläbi isiku õiguste kaitse ning tagades õigusliku regulatsiooni selguse.

Seetõttu ei ole ükski mitteregulatiivne lahendusviis käesoleva küsimuse lahendamiseks võimalik.

IV. Probleemi võimalikud regulatiivsed lahendused ja nende mõjud

8. Välisriigid, mille regulatiivseid valikuid probleemi lahendamiseks on analüüsitud

Detsembris 2016.a EL Kohtu poolt tehtud otsus *Tele 2* kohtuasjas mõjutas oluliselt pea kõiki EL liikmesriike, mistõttu tekkis selge vajadus ühise arutelufoorumi järele. Sellest tulenevalt loodi 2017.a I poolaastal sideandmete säilitamise küsimusele keskenduva töögrupi (*Dapix – Friends of Presidency on Data Retention)*, mille raames EL liikmesriikide ja asutuste esindajad vahetavad oma riikide praktikaid ja arutavad võimalikke lahendusi, et leida asjakohane tasakaal isikute põhiõiguste ja õiguskaitseasutuste vajaduste vahel. Muuhulgas annavad liikmesriigid

ülevaate oma riigi kehtivast õigusraamistikust sideandmete säilitamise valdkonnas. Väljatöötamiskavatsuse koostamise hetke seisuga saab öelda, et EL liikmesriikide lähenemine sideandmete säilitamisele on väga killustatud. Osades liikmesriikides ei ole hetkel kehtivat sideandmete säilitamise raamistikku (nt Holland, Sloveenia, Slovakkia, Saksamaa jt), kuid suuresti on liikmesriigid jätnud jõusse oma õigusnorme (nt Prantsusmaa, Ungari, Horvaatia, Läti, Leedu, Rootsi, Soome, Iirimaa, Poola, Hispaania, Taani, Kreeka jt). Mitmed riigid töötavad hetkel uue regulatsiooni väljatöötamise suunas (nt Rootsi, Saksamaa, Holland). Tähelepanu väärib omakorda ka asjaolu, et kaks EL liikmesriiki, kus varasemalt ei olnud üldse sideandmete säilitamise regulatsiooni (Saksamaa ja Austria) on viimase aja tehnoloogiaarenguid silmas pidades kehtestanud riigisisesed sideandmete säilitamise reeglid (Saksamaal ei ole uus seadus jõustunud, kuivõrd on kohtus vaidlustatud). Belgia jõustas pärast EL Kohtu otsuseid uuendatud sideandmete säilitamise reeglistikku, mis oli riigisiseses kohtus vaidlustatud. Juulis 2018 otsustas Belgia kõrgeim kohus esitada sideandmete säilitamise küsimuses eelotsuse EL Kohtule (väljatöötamiskavatsuse koostamise hetkel ei ole EL Kohus eelotsuse taotluse küsimusi veel avalikustanud, kuid teadaolevalt küsib Belgia kohus EL Kohtult tõlgendust selle kohta, kas ja millistel juhtudel saab riigisisese õiguse kehtestamisel tugineda e-privaatsuse direktiivi artiklile 15 lg 1 ning ühtlasi palub Belgia kohus vastust küsimusele, kas enne uue õigusliku lahenduse väljatöötamist on lubatud ajutiselt säilitada sideandmete säilitamise reeglid, vältimaks õiguslikku ebakindlust.[11] Hetkel võib eeldada, et EL Kohus võtab asja menetlusse 2018.a II pooles ning lahendini ilmselt jõutakse mitte varem kui 2019.a jooksul.

Võimalike Eesti lahenduste kaalumisel on vaadanud üldiselt, kuidas erinevad EL liikmesriigid on hinnanud erinevate lahenduste õigusliku rakendamise võimalikkust (nt sihistatud andmete säilitamine) ning millised lahendused on riikide kehtivas õiguses. Arvestades, et valdkondlikud õigusnormid on pidevas muutumises, ei kajasta Justiitsministeeriumi siinkohal põhjalikult teiste riikide õigusaktide hetkeseisu, kuid vastav ülevaade tuleb koostada õiguslike muudatuste koostamise raames.

Üldiselt võib öelda, et EL liikmesriikide lähenemine sideandmete säilitamisele on üsna ühetaoline ning kõik liikmesriigid püüavad leida lahendusi, kuidas tagada vajalik andmete kättesaadavus õiguskaitseasutustele, kindlustades seejuures isikute põhiõiguste kaitse. Liikmesriigid, kus ei ole hetkel kehtivaid sideandmete säilitamise reegleid, otsivad lahendusi asjakohase raamistiku kehtestamiseks.

Põhjalikumalt tuleb Justiitsministeeriumi hinnangul analüüsida järgnevate riikide õiguslikke lahendusi:

- Soome - kuivõrd osa Eesti sideettevõtjaid on Soome operaatorite tütarettevõtted, on Soomes kehtestatud normide analüüs asjakohane. Soome on läbi viinud põhjalikku analüüsi, milles on leitud, et hetkel kehtiv Soome õigus on kooskõlas proportsionaalsuse põhimõttega ning EL põhiõiguste hartaga.
- Iirimaa - 2014.a Euroopa Kohtu otsus *Digital Rights Ireland* asjas põhineb Iiri õigusel, seega Iirimaal kohtuotsusele eelneval ajal ja praegu kehtivate normide analüüs annab täiendavat ülevaadet kohtuotsuse asjaoludest.
- Rootsi – Euroopa Kohtu otsus *Tele2 Sverige* asjas sai alguse Rootsi eelotsusetaotlusest. Kuna mitmed Eesti sideettevõtjad on ka Rootsi operaatorite tütarettevõtted, on asjakohane analüüsida kohtuotsuse valguses ka Rootsi õigust ning seal võetavaid samme. Rootsi riigisisene analüüs sideandmete säilitamise teemal on läbi viidud 2017.a

[11] Belgia konstitutsioonilise kohtu teave: http://www.const-court.be/public/f/2018/2018-096f-info.pdf

II pooles ning analüüsi käigus on leitud, et Rootsi õigus täidab vajalikul määral EL põhiõiguste hartast tulenevaid nõudeid.[12]

- Prantsusmaa – Prantsusmaa on olnud väga aktiivne osaleja sideandmete säilitamise teemalistes aruteludes ning on osalenud EL Kohtu menetlustes, mistõttu on asjakohane põhjalikumalt hinnata Prantsusmaal kehtivaid õigusnorme.

Lisaks erinevate riikide praktikate ja õigusnormide võrdlusele on Justiitsministeeriumi hinnangul asjakohane arvesse võtta erinevate EL asutuste poolt läbiviidud analüüse (nt Europol, Euroust, Terrorismivastane Koordinaator jt) ning liikmesriikide kohtute antud arvamusi erinevatele õiguslikele lahedustele.

9. Regulatiivsete võimaluste kirjeldus ja nende mõjud

Eesmärk on muuta olemasolev sideandmete säilitamise regulatsioon kriminaalmenetluse seadustikus, tsiviilkohtumenetluse seadustikus, väärteomenetluse seadustikus, elektroonilise side seaduses ning eriseadustes, mis sisaldavad hetkel väga killustatud andmete säilitamise reeglistikku (vt ka väljatöötamiskavatsuse lisa 1). Eesmärk on luua võimalikult selge raamistik, mis võtab arvesse viimastel aastatel aset leidnud õiguslikke arenguid ning kohtupraktikat, kuid samuti arvestab ka tehnoloogilist arengut ning õiguskaitsealaseid vajadusi.

9.1. Kavandatavad muudatused

9.1.1 Sissejuhatus

Eesmärgiks on muuta ESS-i sideandmete säilitamist ja säilitatud andmetele juurdepääsu võimaldamist käsitlevad normid, sätestades seni selgemalt ning täpsemalt andmete säilitamist puudutavad üldreeglid. ESS-s muudetakse andmete säilitamise üldisi põhimõtteid ning nähakse ette andmete senisest täpsem ning valikuline säilitamine.

Justiitsministeeriumi hinnangul tuleb sideandmete säilitamisel selgelt eristada, millistel eesmärkidel andmetöötlus toimub. Sõltuvalt eesmärkidest oleks asjakohane sätestada ka erinevad andmete säilitamise ja kasutamise ulatused. Riive ulatuse proportsionaalsuse hindamisel tuleb arvesse võtta, kas andmetöötlus toimub korrakaitselisel, kriminaalmenetluslikul või riigi julgeoleku tagamise eesmärgil. Seega tuleb selgelt eristada erinevatel eesmärkidel andmete säilitamine ning andmetele juurdepääs, kehtestades erinevad reeglid lähtuvalt andmete säilitamise ja töötlemise eesmärgist.

Justiitsministeeriumi hinnangul tuleb muudatuste tegemisel lähtuda kolmesest jaotusest:

1) andmete säilitamise kohustuse ulatus, sh säilitatavate andmete kategooriad, andmete säilitamistähtaeg, andmete säilitamise eesmärgid;
2) säilitatud andmete kasutamise ulatus, sh millistes menetlustes ja millise perioodi jooksul on lubatud kasutada säilitatud andmeid, milliseid andmeid võib erinevates menetlustes kasutada;
3) andmete säilitamise ja säilitatud andmete kasutamisega seotud põhiõiguste tagatised, sh loamenetlus, andmesubjekti informeerimine, juurdepääsu logimine, samade andmete kasutamine erinevates menetlustes.

Sideandmete säilitamise ja töötlemise osas pööratakse tähelepanu ka andmete, mida sideettevõtjad säilitaksid (ka säilitavad) niikuinii ka ilma seaduses sätestatud kohustuseta,

[12] Vastav pressiteade: https://www.regeringen.se/pressmeddelanden/2017/10/morgan-johansson-tog-emot-betankandet-datalagring--brottsbekampning-och-integritet/

juurdepääsule ja nende kasutamisele ülal toodud eesmärkidel, kuna teatud liiki andmed on sideettevõtjatel vajalikud klientidele teenuste osutamise, arveldamise, lepingute täitmise tagamise, võrguliikluse analüüsi ning teenuste kvaliteedi hindamise ja parandamise eesmärgil. Klientide nõusolekul kasutatakse sideandmeid ka turunduslikel eesmärkidel.

Nagu käesoleval ajal, võiks ka edaspidi lähtuda põhimõttest, et eristada üksikpäringut konkreetse sideseansi, sõnumi vms kohta ning üldisema iseloomuga päringuid. Samal ajal tuleks siiski analüüsida täiendavalt võimalusi üksikpäringu regulatsiooni muutmiseks ning ajakohastamiseks.

Sideettevõtjad säilitavad teatud andmeid igal juhul ärilistel eesmärkidel. KrMS § 215 lg 1 sätestab uurimisasutuse ja prokuratuuri määruste ja nõuete kohustuslikkuse ning JAS § 31 lg 2 annab julgeolekuasutustele õiguse saada füüsiliselt või eraõiguslikult juriidiliselt isikult vajalikku teavet. Arvestades KrMS §-s 215 lg 1 ja JAS §-s 31 lg 2 ettenähtud aluseid andmete pärimiseks, võib kerkida küsimus sellest, kas on üldse vajalik riigi poolt sideettevõtjale ette kohustus selliste andmete säilitamiseks, mida ta juba niikuinii teistel eesmärkidel säilitab. Säilitamiskohustuse saaks ette näha ennekõike nende andmekoosseisude osas, mida sideettevõtja ärilistel eesmärkidel ei vaja. Samas ei ole täna selge, milliseid andmeid sideettevõtjad säilitavad ja kui kaua, samuti võivad andmekoosseisud ja tähtajad sideettevõtjate lõikes erineda. Seetõttu tuleks KrMS, JAS ja ESS vastavate sätete omavahelist koosmõju põhjalikumalt hinnata.

Kuna tehnoloogia areng, sealhulgas telekommunikatsiooni valdkonnas on olnud suhteliselt kiire, siis uue regulatsiooni väljatöötamisel tuleks lähtuda tehnoloogianeutraalsuse põhimõttest ning tehniliste standardite ja terminoloogia asemel kasutada andmete üldkategooriaid, üldisemaid geneerilisi mõisteid, mis kataks ära vajalikud andmed. Uute tehnoloogiate ning standardite lisandumisel ei ole mõistlik muuta kogu aeg seadust ning seetõttu võiks kaaluda tehniliste spetsifikatsioonide ja tingimuste sätestamist madalama taseme õigusaktis.

Päevakorda on tõusetunud ka küsimus seoses uute isikutevahelist sidet võimaldavatele internetipõhiste teenustega, nagu IP-kõned, kiirsõnumid ja veebipõhised e-posti teenused (nn *over-the-topp media services, edaspidi OTT-teenused)*. Käesoleval hetkel ei laiene elektroonilise side seadus (ega selle üheks lähtekohaks olevad EL õigusaktid) OTT-teenuse pakkujatele, kuivõrd algse regulatsiooni väljatöötamise ajal ei olnud veel OTT-teenused sellise kasutusulatusega nagu praegu. Tänapäeval on OTT-teenuse kaudu võimalik teha mitmeid erinevaid tegevusi ning OTT-teenused on asendanud suures ulatuses traditsioonilist sideteenust. Vajadusele hõlmata OTT-teenused uue sidealase regulatsiooniga on osutanud ka Euroopa Komisjon. OTT-teenused on hõlmatud nii uue Euroopa elektroonilise side seadustiku eelnõuga kui ka uue e-privaatsuse määruse eelnõuga (mõlema õigusakti ettepanekud hetkel räägitakse EL-is läbi ning need ei ole veel vastu võetud, kuid elektroonilise side seadustiku eelnõu menetlus on juba Euroopa Parlamendiga läbirääkimiste faasis ning hetkel on OTT-teenused jätkuvalt kohaldamisalas). Sideandmete säilitamise reeglite kohaldamisel OTT-teenustele on mitmeid eeliseid, sealhulgas kõrvaldaks see õigustamatu diferentseerimise nn klassikalise sideteenuse pakkuja ja OTT-teenuse pakkuja vahel ning tagaks seega, et õigusraamistik oleks võimalikult ühtne. Siiski tuleb arvestada, et kuigi erinevate kohustuste kehtestamine tavalise sideteenuse pakkujatele ja OTT-teenuse pakkujatele ei pruugi olla õigustatud, ei ole käesoleval hetkel üldreeglid veel ühtlustustatud kuni Euroopa elektroonilise side seadustiku ülevõtmistähtaja saabumiseni ning e-privaatsuse määruse rakendamiseni, mistõttu praktikas ei ole ilmselt asjakohane viia hetkel ESS-i sisse OTT-teenuse osutajaid puudutavaid muudatusi ning laiendada sideandmete säilitamise kohustust OTT-teenuse pakkujatele. Küll aga tuleb kõnealust küsimust analüüsida ning hinnata sellega seotud probleeme ja võimalusi, leidmaks võimalused vastavate õigusnormide loomiseks hetkel, kui jõustuvad elektroonise side

seadustiku ja e-privaatsuse määruse muudatused, millega OTT-teenuse pakkujad hõlmatakse sideteenuse pakkujatele kehtivate regulatsioonidega.

Sideandmete säilitamise küsimuse analüüsimisega seoses kerkis esile ka küsimus seoses anonüümsete kõnekaartidega. Nimelt anonüümsete kõnekaartide korral ei ole võimalik tuvastada numbri omanikku ning seega on tegemist olukorraga, mida on võimalik ära kasutada ebaseaduslike tegevuste eesmärgil. Paljudes EL riikides ei ole anonüümsete kõnekaartide kasutamine võimalik ning mistahes kõnekaardi soetamine eeldab ostja identifitseerimist (näiteks Belgia, Kreeka, Hispaania, Prantsusmaa jt. Sama plaan on näiteks ka Austrias. Peamiseks põhjuseks on seejuures selline kõnekaartide kasutamise ulatus kurjategijate poolt. ESS-i § 111^1 lõike 2 punkti 10 kohaselt on telefoni- ja mobiiltelefoniteenuse ning telefonivõrgu ja mobiiltelefonivõrgu teenuse osutaja kohustatud säilitama anonüümse ettemakstud mobiiltelefoniteenuse korral teenuse esmase aktiveerimise kuupäeva ja kellaaja ning kärjetunnuse, millest teenus aktiveeriti. Justiitsministeeriumi hinnangul on asjakohane hinnata, kas Eestis oleks samuti mõistlik kaaluda isikustamata (anonüümsetest) kõnekaartidest loobumist ning nõuda kaardi omaniku isiku tuvastamist.

Ühtlasi vajab täpsustamist raamistik, mis käsitleb sideettevõtja poolt päringutele vastamist, sh võib olla praktiline vajadus tagada, et teatud kiireloomulistele päringutele võimalikult kiire vastuse saamist. Hetkel kehtiva ESS § 112 lg 1 kohaselt peavad sideettevõtjad vastama kiireloomulistele päringutele esimesel võimalusel või hiljemalt 10 tunni jooksul. Muude ehk mittekiireloomuliste päringute puhul on vastamise tähtaeg 10 tööpäeva jooksul. Tuleb kaaluda, kas peaks olema tagatud kiirem vastamise tähtaeg kiireloomusliste päringute korral, näiteks terrorismiohu puhul.

Täiendavat analüüsi vajab ka päringute esitamise ja päringutele vastamise kord. Hetkel reguleerib olukord ESS § 112, mille lg 2 sätestab, et järelepärimised esitatakse kirjalikus või elektroonilises vormis, teatud piiratud juhtudel on võimalik ka järelepärimise esitamine suulises vormis (omanikupäringute korral). Samas sätestab ESS § 112 lg 2 viimane lause, et teabe kättesaadavuse võib teha ka kirjaliku lepingu alusel pideva elektroonilise ühenduse tagamise teel. Õigusselguse huvides tuleb selgitada, kuidas toimub teabe edastamine püsiva ühenduse korral ning kuidas sellistel juhtudel on tagatud nõutavate tingimuste täitmine, järelevalve ja andmesubjekti õiguste tagamine, päringute ja saadud teabe dokumenteerimine jt.

9.1.2 Andmete säilitamise ulatus

EL Kohus on kohtuotsuses *Tele* 2 sedastanud, et EL põhiõiguste hartaga ei ole kooskõlas olukord, kus säilitatakse kõikide isikute kõiki andmeid, sh ei tehta erisusi lähtuvalt isikust või näiteks kasutatavast seadmest. Andmete säilitamise diferenteerimisel saaks teoreetiliselt lähtuda järgmistest kriteeriumitest:

- isikuline – andmete säilitamise valiku aluseks on isiku vanus, sugu, rahvus, religioon, varasemate karistuste olemasolu jne;
- geograafiline – andmete säilitamise valiku aluseks on teatud piirkonnad;
- seadmepõhine – andmete säilitamise valiku aluseks on teatud liiki seadmete kasutamine;
- teenustepõhine – andmete säilitamise valiku aluseks on teatud liiki teenuste kasutamine.

Andmete valikulise säilitamise juures on vajalik hinnata selle võimalikkust lähtuvalt erinevatest kriteeriumitest, hoidudes samal ajal isikute diskrimineerimisest ning arvestades sideettevõtjate tehnilisi võimekusi ning valikulise säilitamisega kaasnevaid täiendavaid kulutusi. Esialgselt hinnangul leiab Justiitsministeerium, et andmete säilitamine eespool toodud kriteeriumidest

lähtuvalt ei oleks seatud eesmärgi suhtes efektiivne ning looks eeldusi diskrimineerimiseks ja väärkasutamiseks. Kuigi teoreetiliselt on mõeldav, et statistiliste andmete pinnalt pannakse kokku n-ö keskmise kurjategija profiil ja samuti saaks välja tuua kõrgema kuritegevusega piirkonnad Eestis, oleks selliste kriteeriumite alusel sideandmete säilitamine selgelt diskrimineeriv. Samuti võimaldaks selline süsteem siiski andmete säilitamisest kõrvale hoiduda – nt sidevahend pereliikmete (kes nn profiilile ei vasta) nimele vormistada.

Optimaalne lahendus, mida on arutatud ka EL Nõukogu DAPIX töögrupis, on ilmselt nn piiratud sideandmete säilitamine. S.t erinevate andmekategooriate (asukohaandmed, omanikuandmed, kõneeristused jne) osas kehtestatakse erinevad säilitamis- ja kasutamisreeglid, eesmärgiga tagada reeglite kooskõla EL Kohtu praktikaga. Milliseid andmekategooriad säilitada, sõltub ka andmete olulisusest erinevat liiki menetlustes.

Täiendavalt tuleb kaaluda erinevate tähtaegade kehtestamist erinevatele andmekategooriatele (nt asukohaandmed, andmeliiklusandmed jt). Erinevate tähtaegade kehtestamisel tuleks hinnata erinevate andmekategooriate kättesaadavuse olulisust.

Europol on koostöös EL Nõukogu DAPIX töörühma ning liikmesriikidega kaardistanud andmekategooriaid, mida erinevates menetlustes on tarvis ning hinnanud iga andmekategooriat eraldi. Andmekateooriatele on antud väärtus sõltuvalt tema olulisusest ja vajalikkusest kuritegude uurimisel. Analüüsi tulemusena selgus, et kuigi säilitatavate andmete maht on ulatuslik, et väga raske välja tuua sellised andmed, mis on ebavajalikud ning mille kaotamine ei avaldaks märkimisväärset mõju õiguskatiseasutuste võimalustele kuritegevusevastases võitluses. Näiteks vastamata kõne andmete säilitamine võib esmapilgul näida ebavajalik ning asjakohatu, kuid praktikas kasutatakse vastamata kõnesid ulatuslikult kurjategijate vahelises suhtluses andmaks edasi teavet erinevat liiki tegude kohta. Nii võib näiteks kaks helisignaali tähendada etteantud ülesande täitmist, kolm helisignaali võivad omakorda tähendada, et vajalik on kokkusaamine jne.

Lähtuvalt eelpool nimetatud piiratud sideandmete säilitamise põhimõttest tuleks näha seaduses ette andmete säilitamise kohustus ning andmete kategooriad konkreetsete menetluste ning asutuste suhtes. Arvestades sideandmete olulisust riigi julgeoleku ning põhiseadusliku korra kaitse tagamisel, peaks säilima võimalus andmetele juurdepääsuks kõikidele andmekategooriatele riigi julgeoleku tagamisega seotud menetlustes. Siinkohal on kahtlemata oluline ka hetkel pooleli olev EL Kohtu menetlus asjas 623/17 *Privacy International,* kus arutusel all on e-privaatsuse direktiivi artikli 15 lg 1, sellest tulenevate piirangute ning asjaomaste tõlgenduste kohaldamine riigi julgeoleku valdkonnale, mis on vastavalt EL aluslepingutele väljaspool EL pädevust. Kohtuasjas 623/17 peaks eelduslikult kohtuistung toimuma 2018.a sügise alguses ning lahendit võib ilmselt oodata 2019. esimeses pooles. Selles küsimuses on oluline ka 2018.a juulis Belgia kohtu poolt EL Kohtule esitatud eelotsusetaotlus, mille menetlus on alles algusjärgus. Riigi julgeoleku tagamise osas tuleb Justiitsministeeriumi hinnangul säilitada kõige laiem võimalik volitus kasutada säilitatud andmeid, arvestades kaitstava õigushüve olulisust.

Mõnevõrra erinevalt oleks asjakohane käsitleda sideandmete säilitamist kriminaalmenetluses tõendite kogumise eesmärgil. Siinkohal tuleb esiteks viia sisse diferentseerimine lähtuvalt sellest, millise kuriteo menetlust päring puudutab. Väärteomenetluses tõendite kogumise eesmärgil andmete säilitamine peaks olema omakorda veelgi kitsama kohaldamisalaga, kuivõrd kaitstav õigushüve on madalama tähtsusega. Kriminaalmenetluse korral peab olema tagatud, et menetlejatel on alati võimalik saada juurdepääs teabele, mida sideettevõtjad säilitavad igal juhul oma ärilistel eesmärkidel ning andmete kättesaadavus peab olema kindlustatud kogu perioodi vältel ja kõikide andmete osas, mida sideettevõtja on kogunud teenuse pakkumise

raames kuni vastava tähtaja lõpuni. St kui näiteks sideettevõtja säilitab kõiki andmeid oma teenuse pakkumisega seotud eesmärkidel kolme kuu jooksul, peab kriminaalmenetluses olema võimalik nende kolme kuu jooksul saada juurdepääs kõikidele andmetele. See on kooskõlas ka KrMS § 215 lg-ga 1, mille kohaselt on uurimisasutuse ja prokuratuuri määrused kriminaalmenetluses kohustuslikud. Seega kui sideettevõtjad säilitavad andmeid oma eesmärkidel, peab olema KrMS-st lähtuva üldpõhimõtte kohaselt olema võimalik neid andmeid saada ka kriminaalmenetlusest. Kui seejärel sideettevõtja oma ärilistel eesmärkidel enam mingit kategooriat ei säilita, kuid andmed säilitatakse jätkuvalt kriminaalmenetluse eesmärkidel, peab olema võimalik juurdepääs ainult neile andmetele, mille säilitamise eesmärk on kriminaalmenetlus sõltuvalt kuriteo raskusest (vaatamata sellele, et riigi julgeoleku tagamise eesmärgil jätkuvalt säilitatakse kõiki andmeid pikema perioodi vältel). Sarnaselt tuleb läheneda ka väärteomenetluses andmete kasutamisele, kuid seejuures tuleb kindlalt piiritleda väärteod, mille raames on üldse sideandmete kasutamine lubatud.

Eraldiseisvalt, kuid samast loogikast lähtuvalt tuleb käsitleda andmete säilitamist korrakaitselistel eesmärkidel, sh andmete kasutamist erinevates haldusmenetlustes ja taustakontrollides. Kuigi haldusmenetluses võib andmete kasutamine olla äärmiselt oluline, nt seoses strateegilise kauba loa andmisega, tuleb arvestada kohtupraktikast tulenevaid kitsendusi ning vajadust tagada proportsionaalsuse põhimõte. Seega tuleb kindlustada, et korrakaitselistel eesmärkidel säilitatakse andmeid väiksemas mahus ning lühemaks perioodiks, kui teiste menetluste korral. Siinkohal tuleb analüüsida, kas võimalik lahendus võiks olla eraldiseisva andmete säilitamise regulatsiooni kaotamine korrakaitselistel eesmärkidel ning üksnes selliste andmete kasutamise võimaldamine, mis sideettevõtjal konkreetsel ajahetkel on olemas. Hetkel reguleerib korrakaitselistel eesmärkidel andmete kasutamist KorS § 35, aga ka mitmed eriseadused.

Viimaks tuleb näha ette proportsionaalne raamistik andmete kasutamiseks tsiviilkohtumenetluse tarbeks. Justiitsministeeriumi hinnangul ei ole asjakohane rääkida andmete säilitamisest tsiviilkohtumenetluse eesmärgil, vaid seda küsimust tuleb käsitleda seoses andmetele juurdepääsuga tsiviilkohtumenetluses, näiteks seoses lepinguvälise kahju tekitamisega (nt hea nime teotamine jt) või intellektuaalomandiga seotud vaidlustes. Kuivõrd tsiviilkohtumenetluses esitavad pooled omapoolseid tõendeid, tuleks näha ette raamistik, mille kohaselt on kohtul endal võimalik nõuda sideettevõtjalt teatud andmeid, mida kohus peab konkreetses vaidluses oluliseks. Seejuures saab nõuda üksnes selliseid andmeid, mida sideettevõtja säilitab oma tegevuse raames ning mitte näiteks riigi julgeoleku tagamise või kriminaalmenetluse eesmärgil säilitatavaid andmeid.

Lähtuvalt andmete säilitamise eesmärgist tuleb näha erinevad andmete säilitamise tähtajad. hetkel kehtiv regulatsioon näeb ette üldise kohustuse säilitada kõiki andmeid ühe aasta jooksul alates sideseansi toimumisest. Asjakohane on eristada andmete säilitamise tähtajad lähtuvalt erinevatest andmekategooriatest ning andmete säilitamise eesmärkidest. Näiteks riigi julgeoleku tagamise eesmärgil säilitatavate andmete säilitamistähtaeg peaks olema võimalikult pikk, kuivõrd riigi julgeolekuga seotud ohtude ennetamine, tõkestamine ja menetlemine eeldab võimalikult ulatuslikku juurdepääs teabele pikema aja vältel (kehtiv säilitustähtaeg 1 aasta võib olla isegi liialt lühike). Kriminaalmenetluse korral tuleks eristada, milliseid andmeid säilitatakse mis perioodi jooksul. Sarnast lähenemist kasutab või soovib kasutada näiteks Soome, Rootsi, Ungari.

Kolmandaks tuleks näha ette erinevad reeglid lähtuvalt säilitatavate andmete kategooriast. Väiksema riive ulatusega andmed, näiteks numbri kasutaja andmeid, tuleks säilitada pikema perioodi jooksul kui oluliselt tundlikumaid andmeid, näites asukohaandmeid.

Selline eristamine erinevate andmete säilitamise eesmärkide, andmete kategooriate ja andmete säilitamistähtaegade osas võimaldaks senisest oluliselt paremini tagada säilitamise proportsionaalsust ning seega aitaks kaasa EL Kohtu poolt sedastatud probleemide lahendamisele.

9.1.3 Säilitatud andmete kasutus

Säilitatud andmete kasutamise korral tuleb oluliselt piiritleda, millisel juhtudel on lubatud päringute tegemine erinevates menetlustes. Sarnaselt eelmises punktis kirjeldatuga peaks kõige ulatuslikum kasutamine olema lubatud riigi julgeoleku tagamisel säilitatud andmete korral ning kõige väiksem sellistel juhtudel, kus kaitstav hüve on väiksem.

Näiteks tuleb kindlalt piiritleda, milliste väärtegude menetlemise korral on üldse võimalik sideandmete kasutamine ning milliseid andmeid võib väärteomenetluses kasutada. Kehtiv seadus näeb ette võimaluse sideandmeid teatud tingimustel kasutada ka väärtegude menetlemisel[13]. Siinjuures võiks üheks kriteeriumiks sideandmete kasutamise lubatavusel olla see, et väärtegu on toime pandud sidevahendi vastu või sidevahendi vahendusel. Juhul kui sideandmete kasutamine väärteomenetluses üldse välistada, tähendaks see sisuliselt pea kõikide interneti vahendusel toime pandud varavastaste väärtegude, nt kelmuste uurimise võimatust. Eeskätt oleks andmete kasutamine õigustatud juhtudel, kui konkreetne väärtegu on toime pandud sidevahendi abil ning on piisavalt kaalukas lähtuvalt avalikust huvist ning võimalikust karistusest. Näiteks tuleb põhjalikult kaaluda, kas asukohaandmete kasutamine väärteomenetluses on proportsionaalne ning millistel juhtudel ja vastavad olukorrad seaduses selgelt piiritleda. Igal juhul peaks andmete kasutamine väärteomenetluses olema rangelt erandlik ning selgelt põhistatud.

Kriminaalmenetluse puhul tuleb laiemat kasutamist lubada ennekõike raskete kuritegude korral ning kaaluda päringute tegemise piiramist kergemate kuritegude korral. Ka siin tuleb meeles pidada, et on ka selliseid kuritegusid, mille sanktsioonimäär ei ole kõrge, kuid mille avastamine ja menetlemine muutuks sideandmeteta keeruliseks või võimatuks (nt nn netikelmus).

Haldus- ja tsiviilmenetluse puhul tuleb rangelt ära piiritleda, millistele andmetele on võimalik saada juurdepääs ning millised peavad olema konkreetses menetluses esile kerkinud asjaolud või kahtlused, mis annavad aluse andmete kasutamiseks. Andmete kasutamine peaks olema lubatud ainult väiksemas ulatuses ning lühema aja vältel. Vältida tuleb selliseid üldisi sõnastusi, mis ei võimalda üldse anda hinnangut sellele, milline on normi ulatus ja mõju ning kuidas on järgitud nii EL õigusest kui Eesti põhiseadusest tulenevaid nõudeid põhiõiguste kaitsel. ESS § 114^2 kohaselt on sideettevõtja kohustatud Maksu- ja Tolliametile esitama tema korralduse alusel maksumenetluses tähendust omavate asjaolude kindlakstegemiseks kliendile sideteenuse eest esitatud arve andmed, välja arvatud andmed kasutatud sideteenuse üksikasjade kohta. Seejuures ei tulene õigusnormist, millised andmed on hõlmatud esitatud arve mõistega ning millised andmed on normi kohaldamisalast välistatud. Ühtlasi ei tulene normist, millist asjaolude väljaselgitamiseks andmeid esitatakse ja kuidas neid kasutatakse.

Täiendavalt tuleb kaaluda võimalust piirata selgelt seaduse tasandil, kes on andmesubjektid, kelle suhtes on teatud päringute tegemine lubatud ning milliste kaalutluste alustel. Näiteks tsiviilmenetluses on ilmselt mõistlik üheselt sedastada, kelle kohta käivaid andmeid saab kohus nõuda (eelduslikult eeskätt menetluse osapool), samamoodi peaks sellise raamistiku kehtestamine olema võimalik haldusmenetluse korral. Riigi julgeoleku kaitse ja

[13] Juhindudes VtMS § 31^2 on sideandmete pärimise õigus vaid teatud menetlusasutustel, lõppkasutaja tuvastamiseks või üksikpäringuna ning üksnes siis, kui see on vältimatult vajalik väärteomenetluse eesmärgi saavutamiseks.

kriminaalmenetluse puhul on vastavate reeglite loomine siiski võimatu, kuivõrd need menetlused keskenduvad sageli alles asjaomaste isikute väljaselgitamisele.

Ühtlasi tuleb eelnõu väljatöötamisel analüüsida kasutatavat terminoloogiat ning kindlustada, et läbivalt on kasutusel üheselt tõlgendatavad mõisted. Näiteks lõppkasutaja puhul tuleks sätestada, et tegemist on füüsilise isikuga, kes on andmekaitseõiguse tähenduses andmesubjekt.

9.1.4 Põhiõiguste tagatised

Selleks, et kindlustada proportsionaalsuse põhimõttest kinnipidamist ning isikute põhiõiguste kaitset, tuleb senisest oluliselt rohkem tähelepanu pöörata nii loamenetlusele (st milline asutus ja mis kaalutluste alusel annab loa sideandmete päringu esitamiseks), isiku teavitamisele andmete kasutamisel või selle järgselt kui ka päringute esitamise ja kasutamise dokumenteerimisele ja logimisele. Kriminaalmenetluses on hetkel kasutusel süsteem, mille kohaselt annab loa sideandmete kasutamiseks prokuratuur ning hetkel ei ole Justiitsministeeriumi hinnangul oluline, et kriminaalmenetluses oleks loa andjaks kohus. Küll aga tuleb üle vaadata, kas, kes ja kuidas annab loa andmete kasutamiseks muudes menetlustes (vt ka väljatöötamiskavatsuse lisa 1). Loamenetluse reeglid peaksid olema menetluste lõike võimalikult ühtsed, selged ning võimalikult vähese halduskoormusega.

Lisaks andmete säilitamise ja juurdepääsu puudutavale regulatsioonile, vajab ülevaatamist ka tehtud päringutest isiku teavitamise ning kogutud andmete tutvustamise regulatsioon. Kriminaalmenetluse raames näeb KrMS ette üldised kriminaaltoimiku andmete tutvustamise reeglid, kuid ka kriminaalmenetluses ei pruugi olla tagatud kõigi seotud isikute võimalus teada saada, et nende andmeid on töödeldud. Kindlasti ei saa olla kohane teavitada sideandmete töötlemisest kõiki neid isikuid, kelle telefoninumbrid võivad olla kajastatud kõneeristusel, sest see eeldaks täiendavate andmete töötlemist (telefoninumbri omaniku identifitseerimist, tema kontaktandmete hankimist). Siiski tuleks luua raamistik, mille kohaselt neid isikuid, kelle andmeid töödeldi ja kus on võimalik isiku teavitamine (st on olemas nt isiku nimi jt), teavitatakse andmete töötlemisest kui töötlemise saladuses hoidmise vajadus on ära langenud sõltuvalt menetluse faasist. Vajalik oleks hinnata nende piisavust ning ühtlasi vaadata üle ka teavitamise ja tutvustamise võimalused teiste menetluste jaoks.

Lisaks tuleb reguleerida, kuidas toimub päringute tegemise dokumenteerimine, millised meetmed on vajalikud tõhusa järelevalve teostamiseks ning kuidas pädevad asutused säilitavad andmeid pärast nende kasutamist, millal andmed kustutatakse ja millised reeglid kehtivad andmete edasisele kasutusele. Kõik need tegurid mõjutavad oluliselt andmete kasutamise proportsionaalsuse tagamist, mistõttu peab seaduse tasandil kindlustama, et ei teki andmete õigustamata järelkasutamist või olukorda, kus järelevalvemenetluse raames puudub võimalus välja selgitada, kellele, miks ja mis olukorras andmeid edastati ning kuidas neid andmeid kasutati. Kuivõrd sideandmete kasutamisel võidakse esitada päringuid mitme isiku kohta ning ka selliselt, et kontrollitakse konkreetse telekommunikatsioonimasti piirkonnas viibinud telefoninumbrite omanikke. Näiteks võib see oluline raskete „pimedate“ kuritegude lahendamisel, kui leitakse surnukeha, kuid tõendite kogumisel ei suudeta leida teavet selle kohta, kes võiks olla süüteo toimepanija. Siis võib kasu olla sellest, et kontrollitakse kindlal ajavahemikul, näiteks eeldatava surmaaja perioodil, lähedal viibinud isikuid ning otsitakse seejärel välistamise teel võimalikke teo toimepanijaid. Menetluse raames satub siiski valimisse ka isikuid, kes ei ole kuidagi menetlusega seotud ning seaduse tasandil tuleb kindlustada, et selliseid isikuid puudutav teave kustutatakse kohe kui selgub, et isik ei ole konkreetse menetletava asjaga seotud. Kuigi see on üldine põhimõte, mis tuleneb isikuandmete kaitse õigusest, oleks asjakohane seda üle rõhutada, vältimaks isikute andmete põhjendamatut

töötlemist. Samamoodi tuleb tagada, et näiteks kõneeristuse puhul ei säilitata ega töödelda edasi andmeid, mis puudutavaid selliste kõnede osapooli, kes ei ole konkreetse menetluse kontekstis asjakohased. Nende olukordade senisest selgem reguleerimine tagab, et säilitatud andmete töötlemine oleks täpselt piiritletud konkreetse vajadusega ning toimuks ainult sellistel juhtudel, kui õigusaktidest tulenevalt on selleks olemas põhjendus ning töötlus on proportsionaalne.

Täpsustada tuleb ka reegleid selle kohta, kas õiguspäraselt hangitud sideandmeid on võimalik kasutada muudes menetlustes või peab andmeid pärima igas konkreetses menetluses eraldi.

Tõhusa järelevalve tagamiseks on vaja sätestada reeglid selle kohta, millist teavet tuleb salvestada tehtud päringute kohta, sh peab olema võimalik tuvastada, miks ja millise menetluse raames on päring tehtud, milliseid andmeid päringu raames saadi, kas nõutav luba oli olemas, kas andmesubjekte on teavitatud, kas andmed kajastuvad nt kriminaaltoimikus või on need kustutatud jt. Oluline on ka päringute kohta statistiliste andmete kättesaadavus. Tõhus järelevalve on väga oluline meede andmete kasutamise õiguspärasuse kindlustamiseks.

9.1.5 Sideandmete säilitamisega piirnevad teemad ja lahendust vajavad küsimused

Lisaks eespool käsitletud probleemidele seoses sideandmete kasutamisega on mitmeid teisi valdkondi, kus on vaja kaaluda hetkel kehtivate reeglite muutmist. Mistahes muudatuste tegemisel tuleb kindlustada, et õigusraamistik oleks võimalikult selge ning isikute põhiõigused oleksid tagatud ning võimalikud riived ja väärkasutused minimaalsed.

Siseministeerium on arutelude käigus välja toonud järgmised probleemid:

1) Häirekeskuse tühikõned. Häirekeskus saab igas kuus u 15 000–20 000 kõneühenduse katset, mis kestavad kuni 10 sekundit, kuid mille jooksul keegi ei kõnele või kostuvad tehnilised helid. Enamik nendest kõnedest on tehtud SIM-kaardita seadmetest, mille kasutajat on väga keeruline või võimatu tuvastada. Kõnesalvestiste läbikuulamine on andnud alust arvata, et seade on mingil põhjusel hädaabinumbri 112 valinud automaatselt. Seetõttu pole välistatud, et tulevikus võib mitmesuguseid sideseadmeid kasutada ka pahatahtlikult hädaabinumbri 112 üle koormamiseks ja abivajajate kõnede blokeerimiseks. Olukorra lahendamiseks tuleb esiteks luua võimalus identifitseerida tühikõnede allikas ning teiseks luua õiguslik raamistik, mis teatud rangelt piiritletud juhtudel võimaldaks piirata juurdepääs hädaabinumbrile 112 mittesihipärase ja pahatahtliku kasutamise korral.

2) Hädaabikõneta asukoha määramine kõrgendatud ohu korral. Sideettevõtja, kes osutab telefoni- või mobiiltelefoniteenust, peab ESS-i kohaselt tagama sidevõrgu toimimise nii, et iga sidevõrgu kaudu on tagatud tasuta ühenduse loomine riigisiseste hädaabinumbritega ja Euroopa ühtse hädaabinumbriga 112. Praktikas leiavad aset juhtumid, kus inimese elu ja tervise seisukohalt on operatiivselt vajalik tuvastada isiku asukoht ilma abivajava isiku enda poolt tehtud hädaabikõneta. Tegemist on olukordadega, kus on põhjendatud alus arvata, et esineb kõrgendatud oht4, kuid abivajav isik ei saa teha hädaabikõnet, ei saa kõnedele vastata või ei vasta teadlikult (nt enesetapud). Probleemi lahendamiseks tuleb luua õiguslik raamistik, mis võimaldaks Häirekeskusel reaalajas tuvastada asukoht ilma hädaabi kõneta. Kindlasti peaks sellisel juhul õigusraamistik olema rangelt piiratud sellega, et andmeid võib pärida ainult Häirekeskus ning ainult juhul, kui on kindlaks tehtud kõrgendatud ohu olemasolu.

3) Kasutaja tuvastamine SIM-kaardita kõnede korral. ESS-i § 88 lõike 3 kohaselt peab sideettevõtja, kes osutab telefoni- või mobiiltelefoniteenust, vahetult kõne ühendamise järel tegema Häirekeskusele (hädaabinumbrile 112 helistamise korral) ning julgeolekuasutusele (lühinumbrile helistamise korral) tasuta kättesaadavaks helistaja telefoninumbri ja teabe

helistaja asukoha kohta. SIM- kaardita kõnede korral telefoninumber puudub ning sellisel juhul on seadme asukoha ja selle kasutaja tuvastamiseks oluline rahvusvaheline mobiilside terminalseadme tunnus ehk seadme IMEI-kood.[14] Seega tuleb luua õiguslik raamistik, mis võimaldaks SIM-kaardita kõnede korral selgeks teha seadme IMEI-koodi.

Kuivõrd kõnealused küsimused on seotud sideandmete töötlemise ja säilitamise kohustusega, on asjakohane ka neid teemasid konsultatsioonide ja eelnõu koostamise käigus käsitleda.

9.1.6. Kokkuvõte

Sideandmete õiguskaitse eesmärkidel säilitamise ja kasutamise regulatsiooni korrastamise raames on Justiitsministeeriumi hinnangul vaja koostada eelnõu, millega korrastatakse nii sideandmete säilitamist kui ka kasutamist puudutav regulatsioon. Selleks tuleb muudatusi teha nii elektroonilise side seadusesse, kriminaalmenetluse seadustikku, väärteomenetluse seadustikku, tsiviilkohtumenetluse seadustikku, korrakaitseseadusesse, julgeolekuasutuse seadusesse ning mitmesse eriseadusesse. Muudatusi tuleb teha komplekssselt, et kindlustada regulatsiooni ühetaolisus, selgus ja õiguspärasus.

9.2 Kavandatavate muudatuste mõjud

Sideandmete säilitamise reeglid, säilitatavate andmete kategooriad ning säilitatud sideandmete kasutamise reeglid kriminaal-, väärteo- ja tsiviilkohtumenetluses muutuvad selgemaks ja täpsemaks. Sätestatakse täiendavad piirangud sideandmete säilitamisel ja kasutamisel.

Mõju menetlejatele ja teistele riigiorganitele

Mõju riigiasutuste korraldusele:
Sideandmete päringuid teostavate asutuste jaoks muutub reeglistik vähemkoormavaks ning selgemaks. Mõneti võib kasvada järelevalvet teostavate isikute koormus. Samas võimaldaks detailsem reeglistik päringute teostamise kohta senisest tõhusamat järelevalve teostamist. Käesoleval ajal on sideandmete säilitamise ja kasutamise regulatsioon äärmiselt killustunud ning ebaühtlane. Selgete ja võimalikult ühtlaste reeglite loomine tagab senisest paremat reeglite järgimist ning võimaldab luua kindlad protsessid, mille kohaselt toimub nii päringute esitamine kui andmete kasutamine.
Hetkel on sideettevõtjal kohustus esitada andmed järgmistele asutustele:
- uurimisasutustel, jälitusasutustel, prokuratuuril ja kohtul kriminaalmenetluses vajaliku teabe kogumiseks;
- julgeolekuasutustel põhiseadusliku korra kaitse eesmärgil;
- Andmekaitse Inspektsioonil, Finantsinspektsioonil, Keskkonnainspektsioonil, Politsei- ja Piirivalveametil, Kaitsepolitseiametil ning Maksu- ja Tolliametil väärteomenetluses vajaliku teabe kogumiseks;
- Finantsinspektsioonil väärtpaberituru seaduses sätestatud juhtudel riikliku järelevalve teostamise eesmärgil;
- kohtul tsiviilvaidluste lahendamise eesmärgil;
- jälitusasutustel kriminaalmenetluse väliste toimingute tegemiseks isiku suhtes, kelle puhul on põhjendatult alust arvata, et ta paneb toime kuriteo või isiku suhtes, kes on kuulutatud tagaotsitavaks;
- pädevatel asutustel tausta- ja julgeolekukontrolli teostamise eesmärgil.

[14] *International Mobile Equipment Identity – IMEI* on unikaalne seerianumber, mis identifitseerib üheselt konkreetse seadme (sh seadme mudeli).

Muudatuste järel loodetakse jõuda selgema raamistikuni ning ühtlasi väheneb eelduslikult ka asutuste ring, kellel on õigus päringuid esitada. Siiski peamine positiivne mõju peaks tulema regulatsiooni selgusest, kuigi tuleb tõdeda, et erinevate tegurite täiendav eristamine (nt erinevad säilitamistähtajad, erinevad andmekategooriad) toob omakorda kaasa pikema ja detailsema reeglistiku. Siiski on see vajalik põhiõiguste kaitse kindlustamiseks ning kohtupraktikas välja toodud probleemide lahendamiseks.
Seoses täiendavate loamenetluste sissetoomisega võib suureneda asutuste koormus, kelle ülesandeks on loa andmine. Samas peaks muudatuste tulemusena oluliselt vähenema üldine päringute arv, mis aitab tasakaalustada võimaliku halduskoormuse kasvu.

Mõjud riigi elanikkonnale

Mõju riigi julgeolekule:
Täpsemad sideandmete kasutamise reeglid võimaldavad regulatsiooni paremat rakendamist riigi turvalisuse tagamisel kriminaal- ja väärteomenetluse kaudu. Normide kehtestamisel võetakse arvesse EL Kohtu praktikast tulenevad nõuded, mis annab kindlamad alused sideandmete kasutamiseks piiriülestes menetlustes.
Sideandmete säilitamine ja kasutamine on vajalik siseriikliku julgeoleku ja turvalisuse tagamise eesmärgil, samuti täitmaks rahvusvaheliste lepingutega võetud kohustusi.

Sotsiaalsed mõjud
Kehtiva õigusega võrreldes piiratum regulatsioon sideandmete säilitamise ning kasutamise puhul aitab ühelt poolt paremini tagada isikute õigust privaatsuse ning eraelu kaitsele. Samal ajal toob sideandmete säilitamise ja kasutamise piiramine kaasa selle, et teatud menetlustes (kriminaalmenetlus, väärteomenetlus, tsiviilkohtumenetlus) muutub keerukaks kui mitte võimatuks süüteo toimepannud isiku tuvastamine või tsiviilkohtumenetluses kahju tekitanud isiku tuvastamine.
See tähendab seda, et edaspidi on süüteomenetluses kannatanu või tsiviilkohtumenetluses hageja õigused vähem kaitstud ning kannatanul ei ole enam võimalik saada riigilt oma õigustele piisavalt kaitset, kuna süüteo toimepannud isikut ei ole enam võimalik tuvastada. Süüteomenetluse puhul toob see kaasa suurema lõpetatud menetluste arvu, kuna süüteo toimepanijat ei ole võimalik enam tuvastada.
Kahju hüvitamise nõude esitamisel tsiviilkohtumenetluses ei pruugi nõude täitmine enam olla võimalik, kuna kahju tekitaja isikut ei saa edaspidi sideettevõtjale tehtava päringu abil tuvastada.

Mõjud sideettevõtjatele

Eestis tegutsevatele sideettevõtjatele toovad õiguslikud muudatused eelduslikult teatud rahalist kulu, kuivõrd säilitatavad andmed tuleb senisest oluliselt rohkem diferentseerida. Siiski säilitatakse kõiki samu andmeid, lihtsalt erinevate andmete säilitustähtajad ja juurdepääsutingimused muutuvad. Paratamatult tooksid muudatused kaasa ka vajaduse teha täiendavaid investeeringuid ning kulusid ning kuivõrd tegemist on riigi jaoks vajaliku tegevusega, peaks riik hüvitama sideettevõtjatel seoses süsteemi ümber ehitamisega kaasnevaid kulusid. Hetkel ei ole võimalik prognoosida võimalike muudatuste maksumust.
Sideettevõtjad on juhtinud erinevate ministeeriumide tähelepanu asjaolule, et kehtiv sideandmete säilitamise raamistik ei ole asjakohane ning seega on sideettevõtjate jaoks oluline, et õigusnormid korrastatakse. Konkreetse lahenduste väljapakkumise ja seaduse eelnõu koostamisel tehakse tihedat koostööd sideettevõtjatega.

10. Regulatiivsete võimaluste põhiseadusega ning Euroopa Liidu ja rahvusvahelise õigusega määratud raamid

Kavandatav regulatsioon puudutab eelkõige järgmisi põhiõigusi ja –vabadusi:

- PS § 3 lg 1 – riigivõimu teostatakse üksnes põhiseaduse ja sellega kooskõlas olevate seaduste alusel. Seaduse reservatsiooni põhimõttest tulenevalt ei tohi küsimust, mis olulisuse ja sisu poolest tuleb reguleerida seadusega, reguleerida määruse või muu seaduse alusel antava õigusakti või sõlmitava lepinguga;
- PS § 10 – sotsiaalse ja demokraatliku õigusriigi põhimõtte kohaselt peavad riigivõimu organid austama põhiõigusi ning inimväärikust. Inimväärikuse põhimõtte osaks on see, et isik kaasatakse tema suhtes langetatava otsuse protsessi, see on piisavalt läbinähtav ja tegelikku kaasarääkimist võimaldav;
- PS § 11 – õiguste ja vabaduste piirangud peavad olema demokraatlikus ühiskonnas vajalikud ega tohi moonutada piiratavate õiguste ja vabaduste olemust. Põhiõiguse piiramine muu põhiseadusliku väärtuse kaitseks on eelkõige seadusandja ülesanne (põhiõiguse piirangu proportsionaalsuse kontroll), mis ei välista kitsamalt määratletud kaalutlusõiguse andmist täidesaatvale riigivõimule;
- PS § 13 lg 2 – seadus kaitseb igaühte riigivõimu omavoli eest. Seaduses peab täidesaatva riigivõimu tegevus olema piisavalt täpselt reguleeritud (määratletuse põhimõte), et kohus saab tõhusalt kontrollida täidesaatva riigivõimu tegevuse vastavust seadusele (määratlemata õigusmõisted, abstraktsed koosseisud ning kaalutlusõiguse andmine pole küll välistatud, aga mida intensiivsem on põhiõiguse riive, seda täpsema peab olema seaduse tekst);
- PS § 14 – õiguste ja vabaduste tagamine on nii seadusandliku, täidesaatva kui ka kohtuvõimu kohustus. Seadusandja on kohustatud kehtestama piisavalt määratletud põhiseadusega kooskõlas olevad õigusnormid, täidesaatev võim järgima kehtestatud õigusnorme ning kohtuvõim kontrollima õigusnormide põhiseaduspärasust ja täidesaatva võimu tegevuse vastavust õigusnormidele;
- PS § 19 – vaba eneseteostus tagab isiku vabaduse muuta oma nime, kaitse salajase pealtkuulamise ja salvestamise vastu, õiguse enese kujutisele jms ning osaliselt kattub see PS § 26 eraelu kaitsealaga. Informatsiooniline enesemääramine tähendab õigust ise otsustada, kas ja kui palju tema kohta andmeid kogutakse ja salvestatakse
- PS § 26 – igaühel on õigus perekonna- ja eraelu puutumatusele. Eraelu hõlmab isiku erasfääri, sotsiaalsete suhete ja kehasfääri ning selle kohta mistahes andmeid tekstis, pildis vms viisil, kui need pole kaitstud PS § 33 ja § 43 osana;
- PS § 33 – igaühe kodu on puutumatu ning kellegi eluruumi, valdusse ega töökohta ei või tungida ega neid ka läbi otsida. Kodu mõiste hõlmab lisaks eluruumile, kus inimene alaliselt või peamiselt elab, ka suvilaid ja haagissuvilaid, laiemalt ka ameti- ja äriruume. Kodu puutumatust riivavad lisaks sissetungimisele, läbiotsimisele ja väljatõstmisele ka pealtkuulamis- ja jälgimisseadmete abil eluruumis, valduses või töökohas toimuva jälgimine ilma neisse kohtadesse sisenemata;
- PS § 43 – igaühel on õigus tema poolt või temale posti, telegraafi, telefoni või muul üldkasutataval teel edastatavate sõnumite saladusele. Üldkasutatavaks on sideteenus, mida sideettevõte pakub sideteenuse turul üldistel alustel kõigile isikutele. Kaitstavad on sõnumid, mis ei ole suhtluse osapoolte mõjualas, eesmärgiga kindlustada sõnumi jõudmine puutumatult saatjalt saajale (vahetu suhtlus ja kohale jõudnud sõnumid on § 26 kaitsealas).

Kavandatav regulatsioon puudutab järgmisi rahvusvahelise õiguse või Euroopa Liidu õiguse allikaid:

- Inimõiguste ja põhivabaduste kaitse konventsiooni artikkel 8 – igaühel on õigus sellele, et austataks tema era- ja perekonnaelu ja kodu ning sõnumite saladust;

- Euroopa Liidu põhiõiguste harta artikkel 7 - igaühel on õigus sellele, et austataks tema era- ja perekonnaelu, kodu ja edastatavate sõnumite saladust;
- Euroopa Liidu põhiõiguste harta artikkel 8(1) - igaühel on õigus oma isikuandmete kaitsele;
- Euroopa Parlamendi ja nõukogu 15. märtsi 2006. aasta direktiiv 2006/24/EÜ, mis käsitleb üldkasutatavate elektrooniliste sideteenuste või üldkasutatavate sidevõrkude pakkujate tegevusega kaasnevate või nende töödeldud andmete säilitamist ja millega muudetakse direktiivi 2002/58/EÜ, EÜT 2006, L 105, lk 54;
- Isikuandmete automatiseeritud töötlemisel isiku kaitse konventsioon. - RT II 2001, 1, 3
- Euroopa Parlamendi ja nõukogu määrus (EL) 2016/679, 27. aprill 2016, füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus), *ELT L 119, 4.5.2016, p. 1–88*
- Euroopa Parlamendi ja nõukogu direktiiv (EL) 2016/680, 27. aprill 2016, mis käsitleb füüsiliste isikute kaitset seoses pädevates asutustes isikuandmete töötlemisega süütegude tõkestamise, uurimise, avastamise ja nende eest vastutusele võtmise või kriminaalkaristuste täitmisele pööramise eesmärgil ning selliste andmete vaba liikumist ning millega tunnistatakse kehtetuks nõukogu raamotsus 2008/977/JSK, *ELT L 119, 4.5.2016, lk 89—131*

11. Muudatuste koondmõju ettevõtete ja/või kodanike halduskoormusele

Muudatused võivad tuua kaasa täiendava koormuse sideettevõtjatele, juhul, kui edaspidi peavad nad hakkama andmeid säilitama senisest piiratumal viisil ning valikuliselt.
Olenevalt valitud lahendustest võivad mõjud sideettevõtjatele olla erinevad. Andmete valikulise säilitamise, erinevate andmekategooriatele erinevate tähtaegade sätestamise puhul peavad sideettevõtjad tegema muudatusi oma infosüsteemides. Kuna teatud liiki andmeid peavad sideettevõtjad säilitama tulenevalt võlaõigusseadusest ja raamatupidamise nõuetest, siis erinevate tähtaegade ning andmete kasutamise eesmärkide sätestamine tooks kaasa täiendava töökoormuse ning ressursivajaduse. Lisaks ei pruugi kõik võimalikud andmete säilitamise valikuvariandid olla tehniliselt mõistlikult teostatavad. Kuna sideettevõtjad ei pruugi alati teada, kes on konkreetse telefoninumbri või seadme kasutaja, siis isikulise säilitamise puhul on vajalik esmalt kasutajad tuvastada ning konkreetse numbri või seadmega siduda. Olukorras, kus ühel füüsilisel või juriidilisel isikul võib olla mitmeid erinevaid telefoninumbreid või seadmeid, samuti anonüümsete ettemaksukaartide puhul, tooks kasutajate isikute eelnev tuvastamine ning isikute ja seadmete nimekirja kaasajastamine kaasa väga suure töökoormuse. Samuti nõuaks see täiendavate infotehnoloogiliste arenduste tellimist kõikide sideettevõtjate puhul.

12. Muudatuste rakendamisega seotud riigi ja kohaliku omavalitsuse eeldatavad kulud ja tulud

Muudatuste rakendamine ei mõjuta oluliselt riigi ja kohaliku omavalitsuse eeldatavaid kulusid ja tulusid. Juhul kui luuakse täiendavad loamehhanismid sideandmete kasutamiseks, kasvab luba andvate ja taotlevate asutuste töökoormus.
Samuti võib tekkida küsimus sideettevõtjatele muudatustega kaasnevate kulude täiendavast hüvitamisest. Juhul, kui kavandatavate muudatuste mõjul on vajalikud olulised ümberkorraldused sideettevõtjate töös ning olulised muudatused telekommunikatsiooni- ja sidesüsteemides, siis võib tekkida küsimus kaasnevate kulude hüvitamise kohta. Samas vajab see sellisel juhul eraldi analüüsi ning otsustamist.

13. Edasine mõjude analüüs

Seaduse eelnõu koostamisel on vajalik täiendavalt analüüsida erinevaid valikuvariante sideandmete säilitamise kohustuse sätestamisel, samuti sideandmete kasutamise piiritlemist. Juhul, kui võrreldes seni kehtinud õigusega muutub sideandmete kasutamine erinevates menetlustes piiratumaks, kaaluda võimalusi, kas ja kuidas on andmete puudumist võimalik kompenseerida muude meetmete või menetlustoimingutega. Väljatöötamiskavatsuses esitatud võimalike lahenduste osas saadud tagasiside alusel tuleb koostada õiguslike muudatuste ettepanekud ning analüüsida konkreetsete muudatuste mõjud, mida kajastatakse seaduse eelnõu seletuskirjas. Juhul, kui süüteomenetluses muutub teatud asjaoludel sideandmete kasutamine võimatuks, siis vajadusel näha ette muude menetlustoimingute või jälitustoimingute kasutamise võimalus, mille abil oleks võimalik jõuda soovitud tulemuseni ning et seeläbi hoiduda teatud liiki asjade mitte menetlemisest või alustatud menetluste lõpetamisest ning seeläbi ka täita riigi positiivset kohustust kaitsta isikuid kuritegevuse ning õigusvastase tegevuse eest. Senisest erineva andmete säilitamiskohustuse, sh andmete valikulise säilitamise, erinevate säilitamistähtaegade sätestamine jms toob kaasa vajaduse teha infotehnoloogilisi muudatusi sideettevõtjate infosüsteemides ning see eeldab erinevate sideettevõtjate ja teenuste lõikes tehnilisi analüüse.

V. Kavandatav õiguslik regulatsioon ja selle väljatöötamise tegevuskava

14. Valitav lahendus			
14.1. Töötatakse välja uus tervikseadus		**14.2. Muudatused viiakse sisse senise seaduse struktuuri**	X
14.3. Selgitus	Muudetakse olemasolev sideandmete säilitamise regulatsioon KrMS-s, TsMS-s, VTM-s, ESS-s. Vajadusel täpsustatakse ka muid asjaomaseid õigusnorme teistes seadustes.		
15. Puudutatud ja muudetavad õigusaktid			
Kriminaalmenetluse seadustik, tsiviilkohtumenetluse seadustik, väärteomenetluse seadustik, elektroonilise side seadus			
16. Edasise kaasamise plaan – keda, millal ja kuidas kaasatakse			
Eelnõu väljatöötamise käigus jätkub konsulteerimine sihtrühma kuuluvate asutuste ja sideettevõtjatega.			
17. Põhjaliku mõjuanalüüsi toimumise aeg			
Eraldi põhjalikku mõjuanalüüsi läbi ei viida.			
18. Eeldatav kontseptsiooni (HÕNTE § 1 lg 3) valmimise ja kooskõlastamisele saatmise aeg (kui järgmise sammuna koostatakse eelnõu kontseptsioon)		Kontseptsiooni ei koostata	
19. Eeldatav eelnõu avaliku konsultatsiooni ja kooskõlastamise aeg		2019 algus	
20. Õigusakti eeldatav jõustumise aeg		2020	
21. Vastutavate ametnike nimed ja kontaktandmed	Julia Antonova (613 4916, julia.antonova@just.ee) Markko Künnapu (6 208 200, markko.kynnapu@just.ee)		