EUROOPA
KOMISJON

Brüssel, 24.7.2019
COM(2019) 372 final

KOMISJONI ARUANNE EUROOPA PARLAMENDILE JA NÕUKOGULE

liikmesriikide pangakontodega seotud automatiseeritud keskmehhanismide (keskregistrid või kesksed elektroonilised andmeotsingu süsteemid) omavahelise ühendamise kohta

KOMISJONI ARUANNE EUROOPA PARLAMENDILE JA NÕUKOGULE

liikmesriikide pangakontodega seotud automatiseeritud keskmehhanismide (keskregistrid või kesksed elektroonilised andmeotsingu süsteemid) omavahelise ühendamise kohta

1. Sissejuhatus

Rahapesuvastase direktiivi 2015/849/EL[1] artikliga 32a on ette nähtud, et liikmesriigid loovad 10. septembriks 2020 automatiseeritud keskmehhanismid, nagu keskregistrid või kesksed elektroonilised andmeotsingu süsteemid, mis võimaldavad tuvastada kõik füüsilised või juriidilised isikud, kellel või kelle kontrolli all on maksekontosid, pangakontosid ja hoiulaekaid. Rahapesuvastases direktiivis on määratletud minimaalne teave, mida sellised keskmehhanismid peaksid sisaldama. Samuti on direktiivis sätestatud, et rahapesu andmebüroodel peaks olema neile keskmehhanismidele kiire ja filtreerimata juurdepääs ning teistele pädevatele asutustele peaksid need olema kättesaadavad rahapesuvastasest direktiivist tulenevate ülesannete ja kohustuste täitmiseks. Direktiiv 2019/1153, millega kehtestatakse normid finants- ja muu teabe kasutamise hõlbustamiseks,[2] kohustab liikmesriike määrama kuritegude tõkestamiseks, avastamiseks, uurimiseks ja nende eest vastutusele võtmiseks pädevad riiklikud asutused, kellel peaks olema vahetu, kiire ja filtreerimata juurdepääs minimaalsele teabele, mis on sellistes keskmehhanismides olemas. Nende pädevate asutuste hulka kuuluvad vähemalt kriminaaltulu jälitamise talitused.

Pädevate asutuste juurdepääs pangakontode keskregistritele või andmeotsingu süsteemidele mängib olulist rolli rahapesuvastases võitluses, rahapesu eelkuritegude ja terrorismi vastu võitlemisel, aga ka üldisemalt raskete kuritegude tõkestamisel. Pidades silmas rahapesuvastase võitluse direktiivi ning finantsteabele ja muule teabele juurdepääsu hõlbustamist käsitleva direktiivi eesmärke, muudaks tulevane tervet ELi hõlmav pangakontoregistrite ja andmeotsingu süsteemide ühendamine lihtsamaks nende piiriüleste pädevate asutuste koostöö, mis on kaasatud võitlusse rahapesu, terrorismi rahastamise ja muude raskete kuritegude vastu.

Rahapesuvastase direktiivi artikli 32a lõikes 5 kohustab komisjoni hindama tingimusi, tehnilisi nõudeid ja korda, millega tagatakse automatiseeritud keskmehhanismide turvaline ja tõhus omavaheline ühendamine. Seetõttu hinnatakse käesolevas aruandes erinevaid ELi tasandi IT-lahendusi, mis juba töötavad või on praegu välja töötamisel ning mis võivad olla keskmehhanismide võimaliku omavahelise ühendamise eeskujuks. Mehhanismide ühendamiseks on vaja õigusakti.

[1]Euroopa Parlamendi ja nõukogu 20. mai 2015. aasta direktiiv (EL) 2015/849, mis käsitleb finantssüsteemi rahapesu või terrorismi rahastamise eesmärgil kasutamise tõkestamist ning millega muudetakse Euroopa Parlamendi ja nõukogu määrust (EL) nr 648/2012 ja tunnistatakse kehtetuks Euroopa Parlamendi ja nõukogu direktiiv 2005/60/EÜ ja komisjoni direktiiv 2006/70/EÜ (ELT L 141, 5.6.2015, lk 73).

[2]Euroopa Parlamendi ja nõukogu 20. juuni 2019. aasta direktiiv (EL) 2019/1153, millega kehtestatakse normid finants- ja muu teabe kasutamise hõlbustamiseks teatavate kuritegude tõkestamisel, avastamisel, uurimisel ja nende eest vastutusele võtmisel (ELT L 186, 11.7.2019, lk 122–137).

Käesolevat aruannet tuleks vaadata koos komisjoni riigiülese riskihindamisaruandega,[3] komisjoni aruandega rahapesu andmebüroode kohta[4] ja komisjoni aruandega ELi krediidiasutustega seotud hiljutiste väidetavate rahapesujuhtumite hindamise kohta,[5] mis kõik esitatakse paralleelselt.

2. Praegune seis

2.1. Pangakontodega seotud keskregistrid ja kesksed andmeotsingu süsteemid liikmesriikides

Praegu[6] töötavad pangakonto andmeid sisaldavad keskmehhanismid 15 liikmesriigis[7]. Liikmesriikidelt saadud vastustest ilmneb, et tehnilise lahendusena eelistatakse mõnevõrra rohkem keskregistrit: nimelt on 17 liikmesriigis kasutusel või kavas kasutusele võtta keskregister, samas kui 9 liikmesriiki teatasid, et neil on olemas või kavas kasutusele võtta keskne andmeotsingu süsteem[8]. Samuti eelistatakse süsteeme, mis sisaldavad täiendavaid andmeid lisaks minimaalsele teabele konto profiili kohta, nagu on ette nähtud 5. rahapesuvastase direktiivi artikli 32a lõikega 5 (vastavalt 11 ja 6 vastust)[9].

2.2. ELi süsteemid, mis ühendavad omavahel riiklikke detsentraliseeritud elektroonilisi andmebaase

On mitu ELi projekti, mis tagavad riiklike elektrooniliste andmebaaside detsentraliseeritud ühendamise terves ELis[10]. Käesoleva aruande seisukohast asjakohased IT-süsteemid on järgmised.

Euroopa karistusregistrite infosüsteem (ECRIS) võeti kasutusele 2012. aasta aprillis, et parandada karistusregistri andmeid puudutavat teabevahetust terves Euroopa Liidus[11]. Praegu on kõik

[3]Komisjoni aruanne Euroopa Parlamendile ja nõukogule siseturgu mõjutavate ja piiriülese tegevusega seotud rahapesu ja terrorismi rahastamise riskide hindamise kohta (COM(2019) 370).
[4]Komisjoni aruanne Euroopa Parlamendile ja nõukogule rahapesu andmebüroode vahelise koostöö raamistiku hindamise kohta (COM(2019) 371).
[5]Komisjoni aruanne Euroopa Parlamendile ja nõukogule ELi krediidiasutustega seotud hiljutiste väidetavate rahapesujuhtumite hindamise kohta (COM(2019) 373).

[6]Selles osas olev teave tugineb liikmesriikide vastustele, mis anti neile 2019. aasta märtsis saadetud spetsiaalsele küsimustikule, samuti teabele, mis saadi komisjoni korraldatud ülevõtmise õpikojas 1. aprillil 2019, ja mõjuhinnangu lisale 7, mis on lisatud ettepanekule võtta vastu Euroopa Parlamendi ja nõukogu direktiiv, millega kehtestatakse eeskirjad finants- ja muu teabe kasutamise hõlbustamiseks teatavate kuritegude tõkestamisel, avastamisel, uurimisel ja nende eest vastutusele võtmisel ning tunnistatakse kehtetuks nõukogu otsus 2000/642/JSK (SWD(2018) 114 final).
[7]Belgia, Bulgaaria, Tšehhi, Saksamaa, Kreeka, Hispaania, Prantsusmaa, Horvaatia, Itaalia, Läti, Leedu, Austria, Portugal, Rumeenia, Sloveenia. Slovakkial on olemas keskne andmeotsingu süsteem, mis on praegu siiski kättesaadav vaid kohtuametnikele.
[8]Soome kasutab mõlemat, sest on kasutusele võtmas süsteemi, mis hõlmab mõlemat lahendust. Keskregister kogub asjakohast teavet ühte kesksesse andmebaasi ja hoiab seda seal, samas kui keskne andmeotsingu süsteem sisaldab keskset IT-portaali, mis kogub teavet eri alusandmebaasidest (mida haldavad näiteks finantsasutused).
[9]Liikmesriikidelt saadud vastuste põhjal võib selline lisateave hõlmata teavet konto omaniku sõlmitud finantslepingute kohta või kontoga seoses tehtud tehingute kohta.
[10]Kesksed IT-süsteemid ühe andmebaasiga ELi tasandil (nt Schengeni infosüsteem või viisainfosüsteem) on hindamisest välja jäetud, sest sellised süsteemid ei saa koos toimida varem loodud riiklikult tsentraliseeritud andmebaasidega.
[11]Nõukogu 26. veebruari 2009. aasta raamotsus 2009/315/JSK, mis käsitleb karistusregistrite andmete vahetamise liikmesriikidevahelist korraldust ja andmete sisu, ning nõukogu 6. aprilli 2009. aasta otsus 2009/316/JSK Euroopa karistusregistrite infosüsteemi (ECRIS) loomise kohta raamotsuse 2009/315/JSK artikli 11 kohaldamiseks, mida praegu muudetakse Euroopa Parlamendi ja nõukogu 17. aprilli

liikmesriigid ECRISega ühendatud. ECRIS tagab, et teavet süüdimõistvate kohtuotsuste kohta vahetatakse liikmesriikide vahel ühtsel, kiirel ja ühilduval viisil ning et kohtunikele ja prokuröridele on tagatud mugav juurdepääs põhjalikule teabele asjaomase isiku kuritegeliku tausta kohta[12].

Euroopa mootorsõidukite ja juhilubade infosüsteem (EUCARIS) võimaldab riikidel jagada sõidukeid ja juhilube puudutavat teavet ja muud transpordiga seotud teavet. EUCARIS on mehhanism, mis ühendab liidu mootorsõidukite ja juhilubade registreerimisasutused, mille kaudu on liikmesriikide kontaktpunktide vahel võimalik vahetada teavet sõiduki omaniku ja sõiduki kindlustuse kohta[13].

ELi-ülene maksejõuetusregistrite ühendamine, mis hõlmab kahte erinevat projekti. Süsteemi esimene versioon (IRI 1.0) on Euroopa e-õiguskeskkonna portaalis[14] olnud kättesaadav alates 2014. aasta juulist. See versioon töötati välja prooviprojektina[15] teatud liikmesriikide vabatahtliku osalusega[16]. Teine versioon (IRI 2.0) tugineb määrusele (EL) 2015/848 maksejõuetusmenetluse kohta ja see ühendab omavahel kõigi liikmesriikide (v.a Taani) riiklikud maksejõuetusregistrid. Kõik liikmesriigid peaksid täitma ühendamiseks vajalikud nõuded 2021. aasta juuniks. IRI 1.0 aluseks on turvalised standarditud veebiteenuse sõnumid (SOAPi tunneldus HTTPS-ühenduse kaudu), samas kui IRI 2.0 toetab ka teabevahetust, mis kasutab Euroopa ühendamise rahastu (CEF) eDelivery platvormi[17].

Ettevõtlusregistrite omavahelise ühendamise süsteem (BRIS) on ühendamissüsteem, mis võimaldab ettevõtlusregistritel vahetada piiriülest teavet ühinemiste ja filiaalide kohta ning e-õiguskeskkonna portaali kasutajatel saada mitmekeelset teavet ELi äriühingute kohta. Süsteem on olnud kasutusel 2017. aasta juulist saadik kooskõlas direktiiviga (EL) 2012/17 keskregistrite, äriregistrite ja äriühingute registrite sidestamise osas[18]. BRIS-süsteem kasutab standardsõnumite vahetamiseks Euroopa ühendamise rahastu platvormi eDelivery. Süsteem on detsentraliseeritud ja sellel on keskne komponent (Euroopa keskne platvorm), mis talletab ja indekseerib äriühingute nimesid ja registreerimisnumbreid.

2019. aasta direktiiviga (EL) 2019/884 teabe vahetamise osas kolmandate riikide kodanike kohta ja Euroopa karistusregistrite infosüsteemi (ECRIS) osas.

[12]2019. aasta aprillis võeti vastu uus õigusraamistik, et toetada ECRISt mehhanismiga, mis võimaldab tõhusalt vahetada karistusregistri andmeid kolmanda riigi kodanike kohta, kes on ELi territooriumil süüdi mõistetud. Kolmandate riikide kodanike andmeid sisaldav Euroopa karistusregistrite infosüsteem (ECRIS-TCN-süsteem) on päringutabamusel või selle puudumisel põhinev kesksüsteem, mis sisaldab teavet üksnes süüdi mõistetud kolmanda riigi kodanike identiteedi kohta ja märget selle kohta, millises liikmesriigis nad on varem süüdi mõistetud. Päringutabamuse korral peab teavet taotlev liikmesriik paluma teavet isiku süüdimõistmise kohta olemasoleva ECRIS-süsteemi kaudu ECRIS-TCN-süsteemis märgitud liikmesriigilt (liikmesriikidelt).

[13]Prümi otsuste kohase teenuse õiguslikud alused on nõukogu 23. juuni 2008. aasta otsus 2008/615/JSK piiriülese koostöö tõhustamise kohta, eelkõige seoses terrorismi- ja piiriülese kuritegevuse vastase võitlusega, ning nõukogu otsus 2008/616/JSK, millega rakendatakse otsust 2008/615/JSK.

[14]https://beta.e-justice.europa.eu/246/EN/bankruptcy_amp_insolvency_registers__search_for_insolvent_firms_in_the_eu.

[15]Prooviprojekt viidi ellu Euroopa e-õiguskeskkonna mitmeaastase tegevuskava (2009–2013) (ELT C 75, 31.3.2009, lk 1–12) ja Euroopa e-õiguskeskkonna mitmeaastase tegevuskava (2014–2018) (ELT C 182, 14.6.2014, lk 2–13) alusel.

[16]Praegu osalevad selles Tšehhi, Saksamaa, Eesti, Itaalia, Läti, Madalmaad, Austria, Rumeenia ja Sloveenia.

[17] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eDelivery.

[18]Euroopa Parlamendi ja nõukogu 13. juuni 2012. aasta direktiiv (EL) 2012/17, millega muudetakse nõukogu direktiivi 89/666/EMÜ ning Euroopa Parlamendi ja nõukogu direktiive 2005/56/EÜ ja 2009/101/EÜ keskregistrite, äriregistrite ja äriühingute registrite sidestamise osas (ELT L 156, 16.6.2012).

Kinnistusraamatute omavaheline ühendamine (LRI) on käimasolev vabatahtlik projekt,[19] mille eesmärk on luua üks pääsupunkt Euroopa e-õiguskeskkonna portaalis osalevate ELi liikmesriikide kinnistusraamatutele. See peaks alustama tööd 2020. aasta teises kvartalis.

European Business Ownership and Control Structures (EBOCS) on projekt, mida viib ellu Euroopa ettevõtlusregistrite ühendus, kes on saanud rahalist toetust sisejulgeolekufondi (ISF) politseikoostöö rahastamisvahendist (2016. ja 2018. aasta tööprogrammid). EBOCS-platvorm tagab lihtsa ja ühtse juurdepääsu äriregistri andmetele äriühingu omandi ja kontrollistruktuuride kohta finantsanalüüsi ja uurimise eesmärgil. Samuti koondatakse päringute tulemused visuaalselt kaardile. Tuleb tähele panna, et Euroopa Liit ei oma selle süsteemi intellektuaalomandi õigusi.

e-CODEXi süsteem (*online* andmevahetus e-õiguskeskkonnas) hõlbustab turvalist sidet tsiviil- ja kriminaalmenetluses, tagades detsentraliseeritud süsteemi piiriüleseks elektrooniliseks sõnumivahetuseks õigusvaldkonnas[20]. e-CODEX hõlbustab praegu elektroonilist suhtlust kodanike ja kohtute vahel ning nende liikmesriikide ametiasutuste vahel, kes osalevad Euroopa maksekäsumenetluse ja Euroopa väiksemate kohtuvaidluste menetluse katsetamisel. Kriminaalõiguse valdkonnas on e-CODEX samuti eelistatud lahendus elektrooniliste tõendite digitaalse vahetussüsteemi (*e-Evidence Digital Exchange System*)[21] jaoks ning elektrooniliseks teabevahetuseks Euroopa uurimismääruse (EIO) ja vastastikuse õigusabi lepingute kontekstis.

3. Põhiparameetrid

3.1. Kasutajate juurdepääsutingimused

Kui vaadata olemasolevaid süsteeme, on ilmne, et sellise lõpptarbijatele mõeldud süsteemi juurdepääsetavus, mis suhtleb ühendatud IT-süsteemiga, sõltub süsteemi eesmärgist. Kui omavaheline ühendus loodi eesmärgiga suurendada siseturul teabe läbipaistvust ettevõtete jaoks (BRIS, IRI), on süsteem avalikult juurdepääsetav. Kui omavahelise ühenduse eesmärk on parandada piiriülest koostööd õiguskaitse valdkonnas tegutsevate pädevate asutuste vahel või avaliku halduse eesmärgil, näiteks ECRISe või EUCARISe Prümi teenuse[22] puhul, on juurdepääs piiratud.

BRIS-süsteemi äriühingu otsimise funktsioon on Euroopa e-õiguskeskkonna portaalis kättesaadav kõigile, samas kui sõnumite saatmine süsteemis on praegu seadusega lubatud üksnes riikide äriregistritele. IRI puhul on teave otsiliidese kaudu avalikult kättesaadav ja ainult tarbija maksejõuetuse menetluse raames on liikmesriikidel võimalik piirata juurdepääsu nii, et selle saavad üksnes õigustatud huvi omavad teabenõude esitajad. ECRISele pääsevad ligi ainult liikmesriikide määratud keskasutused. Samamoodi on juurdepääs EUCARISe teenustele avatud avaliku sektori asutustele määratud riiklike kontaktpunktide kaudu. EBOCSi puhul on juurdepääs piiratud projektis osalevate kuritegevuse vastu võitlemise asutustega.

[19]Selle ühendamise jaoks puudub õiguslik alus, kuid see toimib vabatahtliku süsteemina, mille puhul liikmesriigid saavad otsustada, kas nad osalevad selles või mitte.

[20]e-CODEXi süsteem koosneb tarkvaratoodete paketist (Euroopa ühendamise rahastu platvorm eDelivery ja e-CODEXi ühendusvahend), mida saab kasutada selleks, et luua riiklikul tasandil pääsupunkt turvalise side jaoks. Tegemist ei ole süsteemiga, mis ühendab riiklikke andmebaase või registreid, vaid sidetaristuga, mis tagab turvalise side ja teabevahetuse riiklike IT-süsteemide vahel, ning sellisena peetakse seda käesolevas aruandes hindamise seisukohast asjakohaseks. 21 liikmesriiki töötasid e-CODEXi teiste riikide/territooriumite ja organisatsioonide osalusel välja aastatel 2010–2016.

[21]Süsteemi loomise aluseks olid nõukogu 9. juuni 2016. aasta järeldused küberruumi käsitleva kriminaalõigussüsteemi parandamise kohta.

[22]EUCARISele pääsevad ligi paljud ametiasutused, kuid juurdepääs EUCARISe Prümi teenusele on ette nähtud õiguskaitseasutustele.

Süsteem	Avalik ligipääs	Piiratud ligipääs	Märkused
BRIS	Jah		BRIS-süsteemi äriühingu otsimise funktsioon on Euroopa e-õiguskeskkonna portaalis kättesaadav kõigile, sõnumite saatmine süsteemis on praegu seadusega lubatud riikide äriregistritele.
IRI	Jah		
ECRIS		Jah	Liikmesriikide keskasutustele, mis on selle funktsiooni jaoks konkreetselt nimetatud
EUCARIS		Jah	EUCARISe riiklikele kontaktpunktidele, mille kaudu avaliku sektori asutused saavad juurdepääsu olenevalt koostöö õiguslikust alusest
EBOCS		Jah	Projektis osalevatele kuritegevuse vastu võitlemise asutustele
LRI	Jah*		Lisafunktsioone saavad kasutada üksnes autenditud õigusala töötajad

Tabel 1. Juurdepääs lõpptarbijatele mõeldud süsteemile, mis suhtleb ühendatud IT-süsteemiga

Rahapesuvastase direktiivi alusel on pangakontode keskmehhanismide eesmärk parandada võitlust rahapesu ja terrorismi rahastamise vastu ning juurdepääs neile on piiratud teatud avaliku sektori asutustega. Finants- ja muu teabe kasutamise hõlbustamise direktiiviga on keskmehhanismides leiduva teabe kasutamise eesmärki laiendatud, nii et selleks võib olla võitlus raskete kuritegudega ja juurdepääsuõiguse võivad saada määratud pädevad asutused. Nende riiklike ametiasutuste ring, kellel on otsene juurdepääs liikmesriikide registritele, jääb registreid pidavate liikmesriikide otsustada. See võib tuua kaasa erinevusi, sest teatud tüüpi asutused võivad saada juurdepääsu ühes liikmesriigis, kuid teises mitte. Piiriüleses teabevahetuses tervet ELi hõlmava ühendussüsteemi kaudu võib see tuua kaasa olukorra, kus ametiasutus palub teavet mõne sellise liikmesriigi registrist, kus päringud on sarnasele asutusele keelatud.

Üks võimalus võiks olla see, et ühendamise platvormile saavad juurdepääsu needsamad asutused, kellele antakse otsene juurdepääs keskmehhanismile kooskõlas rahapesuvastase võitluse direktiiviga ja direktiiviga, millega hõlbustatakse juurdepääsu finants- ja muule teabele. Teine võimalus oleks see, et juurdepääsuõigused ühendussüsteemile antakse kõigis liikmesriikides sama liiki ametiasutustele ning seda oleks võimalik saavutada ELi tasandi ühtlustatud ja suletud nimekirjaga sellist liiki asutustest, mis määratakse kindlaks vastavalt sellele, mis eesmärgil asutused juurdepääsu vajavad.

Juhul, kui juurdepääsuõigusi laiendatakse kõigile ametiasutustele, kellele praegu liikmesriikide õiguse alusel juurdepääs antakse, peavad pädevad riiklikud ametiasutused kehtestama üksikasjalikud sätted juurdepääsu ja päringu tegemise tingimuste kohta. Seoses sellega on oluline esile tõsta, et direktiivis finants- ja muu teabe kasutamise kohta on sätestatud liikmesriigi tasandil määratud pädevatele asutustele ranged tingimused, mis reguleerivad juurdepääsu automatiseeritud keskmehhanismis sisalduvale pangakontot puudutavale teabele ja vastavate päringute tegemist. Näiteks üks tingimus on, et juurdepääsu registritele ja andmeotsingu süsteemidele tohib anda üksnes asjaomase pädeva asutuse spetsiaalselt määratud ja volitatud isikutele. Teine meede, mis aitab leevendada riske, mida juurdepääsuõiguste laiendamine liikmesriigi määratud ametiasutuste poolt endast kujutab, on ühendatud süsteemis kättesaadava teabe ulatuse piiramine konto profiili puudutava minimaalse teabega, nagu on sätestatud rahapesuvastase võitluse direktiivi artikli 32a lõikes 3.

* Ei ole veel kasutusel

Mis puutub teabe ulatusse, siis rahapesuvastase võitluse direktiivi artikli 32a lõikes 3 on määratletud teave, mida kõik kesksed süsteemid peavad sisaldama, sh konto omanik, IBAN-numbriga pangakontod ja liikmesriigi territooriumil asuvas krediidiasutuses omatavad hoiulaekad. Direktiivi artikli 32a lõikega 4 on aga ette nähtud võimalus, et liikmesriigid lisavad registrisse muud teavet, mida peetakse rahapesu andmebüroode ja pädevate asutuste jaoks esmatähtsaks nende direktiivist tulenevate kohustuste täitmiseks. Isikuandmete kaitse seisukohast näib olevat vajalik, et teave, millele on võimalik ühendusplatvormi kaudu juurde pääseda, piirduks minimaalse kohustusliku teabega, nagu on määratletud rahapesuvastase võitluse direktiivi artikli 32a lõikes 3. Kooskõlas andmekaitse-eeskirjadega peaks juurdepääs isikuandmetele olema proportsionaalne sellega, mis on vajalik rahapesuvastase võitluse direktiivis määratletud eesmärkide saavutamiseks. Samasugune lähenemisviis on võetud direktiivis finants- ja muu teabe kasutamise kohta. Selle direktiivi artikli 4 lõikes 2 on selgitatud, et lisateave, mille liikmesriigid keskmehhanismidesse lisavad, ei ole pädevatele asutustele juurdepääsetav ega päringuteks avatud.

3.2. Otsingufunktsioon

Kohaldatavad otsingukriteeriumid on olulise tähtsusega tagamaks, et automatiseeritud keskmehhanismide ühendamine tooks kasutajatele lisaväärtust. Otsingukriteeriumid peaksid olema kavandatud selliselt, et need aitaksid asjaomastel ametiasutustel paremini täita oma ülesandeid ja teha uurimisi tõhusamalt, tagades samal ajal proportsionaalsuse ja austades kohaldatavaid andmekaitsenõudeid.

Kaaluda tuleks seda, kellele antakse õigus päringuid teha (eraisikud või avalik-õiguslikud isikud) ja milliseid andmeid on või ei ole võimalik eelduste kohaselt pidada päringut tegeva isiku jaoks teada olevaks. Kui kehtestatakse nõue, mille kohaselt peaks päring sisaldama andmeid, mis ei ole päringut tegeva isiku jaoks tõenäoliselt teada, võib see muuta tõhusate päringute tegemise keeruliseks või võimatuks. Samuti tuleb märkida, et on juhtumeid, kus ühe liikmesriigi rahapesu andmebüroo või õiguskaitseasutus ei ole teadlik mõne teise liikmesriigi kodaniku sünnikuupäevast või isikukoodist. Juhul, kui ühendamisega tehakse juurdepääsetavaks ka selline keskses süsteemis sisalduv lisateave, on oluline kindlaks määrata, kas ka sellise lisateabe alusel on võimalik päringuid teha.

Otsingukriteeriumitena võib ette näha teabeliigid, mis moodustavad ühtlustatud miinimumteabe rahapesuvastase võitluse direktiivi artikli 32a lõikes 3. See muudaks ühendussüsteemi vastavaks keskmehhanismide algsele eesmärgile. Vaja oleks täiendavaid kaitsemeetmeid, mis võimaldaksid kontrollida päringutabamusi (eriti siis, kui päringu tulemuseks on mitu vastet).

Ühendatud andmebaaside kasutamise tõhususe seisukohast on võimalus teha erinevaid otsinguid otsustava tähtsusega. Võimalus teha hägusotsingut, st päringuid, mis annavad rohkem tulemusi isegi siis, kui sõna on valesti või poolikult kirjutatud, annab rohkem tabamusi, suurendades seeläbi tõenäosust jõuda päringuga otsitava teabeni, kuid samas võib see tekitada andmekaitsega seotud probleeme, sest päringuga võidakse paljastada isikuandmed, mida päring algselt ei puudutanud. Seevastu täpse vaste nõue vähendab isikuandmete tarbetu avaldamise ohtu, kuid suurendab tõenäosust, et otsimootor ei leia otsitavat teavet (juhul kui kirje kirjapilt erineb või kui kasutatakse teistsuguseid transliteratsioonireegleid).

Võimalus teha hägusotsingut vähendaks automaatsete valideerimismenetluste kasutamist ja aitaks seeläbi vältida või vähendada ekslike tabamuste mahtu, kuid samas kahandaks see ka süsteemi operatiivset väärtust. Hägusotsingu puhul tuleks kaaluda teisi vahendeid selgelt sihipäratute otsingute riski leevendamiseks. Näiteks IRI puhul on kuvatavate tulemuste arvule seatud ülempiir.

3.3. Juhtimisstruktuur, vastutus haldamise eest

BRISi, IRI, LRI ja ECRISe puhul vastutavad Euroopa Komisjoni eri talitused *IT-süsteemi haldamise eest*, st nad peavad tagama ühendamiskomponendi kättesaadavuse, ning kannavad süsteemi kasutusele võtmise ja haldamise kulud. Praegu haldab e-CODEXi süsteemi liikmesriikide konsortsium (Euroopa ühendamise rahastu eDelivery komponent kuulub Euroopa Komisjoni haldusalasse). EUCARISe puhul kannavad vastutust 28 liikmesriiki ja osalevad kolmandad riigid, samas kui EBOCSi puhul on süsteemi omanik Euroopa ettevõtlusregistrite ühendus (*European Business Registers' Association*, EBRA). Kuna need IT-süsteemid ühendavad riiklikke andmebaase, lasub vastutus riiklike andmebaaside haldamise ja nende kättesaadavuse tagamise eest liikmesriikidel.

Andmebaase ühendava süsteemi *juhtimisstruktuuri* puhul peaks pädevus poliitiliste ja tegevusega seotud otsuste tegemise eest olema korraldatud selliselt, et see teeniks liikmesriikide komponentide huvisid.

BRISi puhul on BRISi juhtkomitee komisjonisiseseks foorumiks, kus võetakse vastu poliitilisi otsuseid, tehakse järelevalvet BRISi üle ja juhitakse seda, samas kui äriühinguõiguse eksperdirühm äriregistrite alal (CLEG-BRIS) on foorum, kus toimub kaasatud osalejate vaheline poliitikatasandi koostöö. Samamoodi eristatakse poliitikakujundamis- ja operatiivstruktuure ka EUCARISes, kus valitsusasutuste kõrgetest esindajatest koosnev peaassamblee võtab vastu poliitilisi otsuseid, kinnitab eelarve ja iga-aastased osamaksed ning annab korraldusi süsteemi juhtimise kohta.

3.4. Vastutus andmete eest

Vastutus IT-süsteemi haldamise eest erineb *vastutusest andmekaitse eest*. Isikuandmete kaitse üldmääruse[23] kohaselt on vastutav töötleja füüsiline või juriidiline isik, kes määrab üksi või koos teistega kindlaks isikuandmete töötlemise eesmärgid ja vahendid ning kannab vastutust isikuandmete töötlemise eest. Vastutuse teema on keeruline ja vastutava töötleja hindamisel tuleb arvesse võtta paljusid tegureid, sealhulgas seda, kes andmeid hoiustab ja kus.

Mis puutub IRIsse, siis ELi platvorm ühendab üksnes liikmesriikide detsentraliseeritud andmebaasid ning kõik kesksel platvormil kuvatud andmed on lihtsalt nn seansiandmed, mida ei salvestata ELi komponendis, nii nagu ei salvestata ega hoita keskselt ka kasutajate poolt veebiteenuse kaudu salvestatud päringute logisid. Olukord on mõnevõrra erinev BRISi puhul, milles võeti kasutusele funktsioon salvestada ettevõtete olulisi profiiliandmeid komisjoni tasandi kesksesse komponenti, mida liikmesriikide registrid korrapärase intervalli järel ajakohastavad. Algne päring tehakse selles keskses andmebaasis ning tulemuseks on päringutabamuste nimekiri koos üksuste nimedega. Teabenõude esitaja võib saada üksikasjalikke andmeid konkreetse üksuse kohta, valides selle üksuse nime vastuste nimekirjast, ning selle toiminguga luuakse otsene ühendus liikmesriigi andmebaasis oleva teabega.

Seoses keskmehhanismide võimaliku omavahelise ühendamisega tuleks kaaluda ka sellise IT-süsteemi loomist, milles keskne marsruutimiskomponent ei salvesta mingeid isikuandmeid ning milles kõik otsused andmetöötluse vahendite ja eesmärkide kohta tehakse liikmesriigi tasandil. Ühendamisteenuse eesmärk oleks lihtsalt andmetöötluse hõlbustamine keskmehhanismide jaoks, mis jääksid samas nende vastavate andmekogumite vastutavaks töötlejaks.

[23]Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta määrus (EL) 2016/679 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).

3.5. Loomis- ja halduskulud

Liikmesriikide keskmehhanisme ühendava süsteemi sisseseadmine tekitab kulusid nii süsteemi loomise kui ka selle haldamise seisukohast ning need kulud tuleb jagada ELi ja selle liikmesriikide vahel. Vaadates kulude jagamist näidismudelite puhul, siis enamasti rahastati ELi komponendiga seotud kulusid (keskne marsruutimiskomponent, ELi platvorm) ELi üldeelarvest, samas kui liikmesriigid kandsid kulud, mis olid vajalikud nende enda riiklike süsteemide kohandamiseks, et muuta need ELi ühendussüsteemiga koostalitlevaks. BRISi puhul kulus esimese, 2017. aasta juunis kasutusele võetud ja Euroopa keskset platvormi hõlmanud versiooni väljatöötamiseks ligikaudu 1,7 miljonit eurot. Lihtsama arhitektuuriga IRI puhul küündisid keskse otsingusüsteemi katseversiooni (IRI 1.0) arendamise kulud ligikaudu 280 000 euroni, samas kui keskse otsingurakenduse kohandamine IRI 2.0 eel maksab ligikaudu 170 000 eurot. ECRISe puhul oli tarkvara Reference Implementation, mis võimaldab liikmesriikidel vahetada karistusregistri andmeid, kasutusele võtmise kogukulu 2 050 000 eurot. Süsteemi haldamise aastakulu oli 150 000 eurot. EUCARISe puhul küsitakse igalt osalevalt riigilt üldist hooldustasu, mis on umbes 20 000 eurot.

Ülaltoodud arvudest ilmneb, et kogu ELi hõlmava ühendamissüsteemi kasutusele võtmise ja haldamise kulu on suhteliselt väike võrreldes sellega, millist kasu selline projekt ELi jaoks kaasa toob. Kulutõhusust oleks võimalik parandada olemasoleva suutlikkuse taaskasutamise kaudu (näiteks eDelivery pääsupunktid, Euroopa ühendamise rahastu elemendid, Euroopa Komisjoni informaatika peadirektoraadi põhisõnastikud jne).

4. Süsteemide, sh andmeturbe tehniline kirjeldus

4.1. Kasutatav võrk ja andmeturve

EUCARISe ja ECRISe Prümi teenus kasutab privaatvõrku *Trans European Services for Telematics between Administrations* (TESTA), mis on avalikust internetist täielikult eraldiseisev võrk. Liikmesriikide määratud kontaktpunktidel on juurdepääs sellele privaatvõrgule. TESTA võrguteenust käitab komisjon ning see tagab garanteeritud jõudluse ja turvalisuse väga kõrge taseme. EUCARISe kasutamine avaliku interneti kaudu on võimalik, kuid praegu seda ei rakendata. Sellel on ühendused kõigi ELi institutsioonide ja liikmesriikide võrkudega ning seda eelistatakse tundlikku teavet hõlmava õiguskaitsealase koostöö kontekstis. ELi institutsioonid on välja töötanud ka teisi turvalisi võrkusid, näiteks ühine teabevõrk / ühine süsteemiliides (CCN/CSI), mis on kasutuses tolli ja maksustamise valdkonnas.

BRIS, IRI, LRI ja EBOCS kasutavad avalikku internetti (koos asjakohase krüptimistehnoloogiaga võrgu kaudu liikuvate andmete jaoks). Mis puudutab avalikus internetis toimuvat turvalise teabevahetust ,siis eDelivery platvorm võimaldab ettevõtetel ja riiklikel haldusasutustel vahetada elektroonilisi andmeid ja dokumente teiste organisatsioonidega digitaalsel kujul ning koostalitleval, turvalisel, töökindlal ja usaldusväärsel viisil. See on kooskõlas e-andmevahetusteenuse (ERDS) määratlusega eIDASe määruse artikli 3 lõikes 36[24].

Selliste kesksete süsteemide võimalikuks omavaheliseks ühendamiseks, mis väidetavalt sisaldavad tundlikku teavet, võiks ette näha TESTA kasutamise. Sellegipoolest võib kaaluda ka avaliku interneti lahendusi. Peaaegu kõik liikmesriikide kesksüsteemid kasutavad avalikku internetti. Andmete turbe ja

[24]Euroopa Parlamendi ja nõukogu 23. juuli 2014. aasta määrus (EL) nr 910/2014 e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul ja millega tunnistatakse kehtetuks direktiiv 1999/93/EÜ (ELT L 257, 28.8.2014, lk 73–114).

tervikluse seisukohast leevendab asjaolu, et süsteem koosneb detsentraliseeritud andmebaasidest, võimalikke riske, sest detsentraliseerimine ja hajustehnoloogiad on juba iseenesest küberrünnetele vastupidavamad, sest andmeid on palju raskem üldisemas ulatuses rikkuda ja neid on pärast intsidente palju lihtsam taastada.

4.2. Keskne marsruutimiskomponent

IT-süsteemid jagunevad arhitektuuri seisukohast kahte liiki, st täielikult detsentraliseeritud süsteemid ja need, millel on ELi tasandil kasutatav keskne platvorm või marsruutimiskomponent, mis toimib liikmesriikide detsentraliseeritud andmebaaside ühendajana.

Nn läbinisti hajussüsteemidel puudub ELi platvorm või komponent, kuid kõik riigid suhtlevad vahetult üksteisega, võttes appi ühiselt kokkulepitud standardid, mis võimaldavad vahetut kolleegidevahelist teabevahetust liikmesriikide ühendatud punktide vahel. Seega suunatakse käivitatud päring eraldi iga teise liikmesriigi süsteemi ning saadud vastused kogutakse kokku ja kuvatakse läbi teabenõude esitaja veebikliendi. Sellist tehnilist lahendust kasutavad EUCARIS, ECRIS ja e-CODEX (tuginedes ühiselt välja töötatud rakendusele).

Keskse marsruutimiskomponendiga hajussüsteemidel on ELi tasandil olemas keskne platvorm: üks keskne veebiteenus, mida hallatakse ja juhitakse ELi tasandil ja mis on ühendatud kõigi riiklike süsteemidega. Kasutajad esitavad päringuid tsentraalse veebiteenuse kaudu, mis kogub teavet liikmesriikide andmebaasidest. Seda tehnoloogiat kasutavad BRIS, EBOCS ja IRI[25].

Keskse marsruutimiskomponendiga lahendust on ühenduvuse seisukohast võib-olla lihtsam rakendada. Kui on ainult üks ühine platvorm, peab iga liikmesriik looma vaid ühe ühenduse liikmesriigi süsteemi ja asjakohase keskse platvormi vahel ning seda haldama. Nn reaalse keskse platvormi puudumise korral peab iga liikmesriik aga looma ühenduse kõigi teiste liikmesriikide riiklike süsteemidega ning neid katsetama ja haldama (nt EUCARISe Prümi teenusel on praegu ligikaudu 756 ühendust). Läbinisti hajussüsteemi puhul tuleb toime tulla mitmekordse ühenduste arvuga ning see võib suurendada juhtimise, kontrollimise ja järelevalve probleeme. Samas on olemas ka tehnoloogilised lahendused, mis aitavad lahendada suure arvu võimalike ühenduste juhtimise probleemi. Samal ajal tuleb arvesse võtta asjaolu, et keskse marsruutimiskomponendiga süsteemi puhul võib kesksest komponendist saada terve süsteemi nõrk lüli.

4.3. Andmevahetusprotokoll

BRIS ja e-CODEX kasutavad Euroopa ühendamise rahastu eDelivery lahendust, samas kui IRI 2,0 kasutab nii Euroopa ühendamise rahastu eDelivery kui ka SOAPi[26] sidet. EUCARISe Prümi teenus ja EBOCS kasutavad SOAPi-põhiseid liideseid. LRI rakendab RESTfuli veebiteenuseid[27].

Euroopa ühendamise rahastu eDelivery platvorm aitab kasutajatel vahetada üksteisega elektroonilisi andmeid turvalisel, töökindlal ja usaldusväärsel viisil. eDelivery lahendus tugineb hajutatud mudelile nimega *4-corner model*, milles kasutajate tagarakendussüsteemid ei vaheta andmeid otseselt

[25]Kesksel komponendil on ka alternatiivid. Näiteks Euroopa ühendamise rahastu eDelivery *Service Metadata Publisher* (SMP) võimaldab sõnumivahetuse infrastruktuuri osalejatel jooksvalt üksteise suutlikkust (juriidilist, korralduslikku ja tehnilist) tuvastada. Sellise hajusarhitektuuri tõttu on igal osalejal vaja kordumatut tunnust. Keskne komponent *Service Metadata Locator* (SML) kasutab neid tunnuseid selleks, et luua veebiaadressid, mis teisendamise korral suunavad eDelivery pääsupunktid osalejat puudutava konkreetse teabe juurde.

[26]Lihtne objektipöördusprotokoll (*Simple Object Access Protocol*).

[27]*Representational State Transfer* on tarkvaraarhitektuuri stiil, mis määratleb teatavad piirangud, mida tuleb veebiteenuste loomisel kasutada.

üksteisega, vaid pääsupunktide kaudu. Need pääsupunktid vastavad samadele tehnilistele kirjeldustele ja on seega suutelised omavahel suhtlema. eDelivery üheks eeliseks on ka see, et see tagab eri pääsupunktide vahelise andmevahetuse turvalisuse, ilma et oleks vajadust spetsiaalse arenduse järele. Selle tulemusel saavad kasutajad, kes võtavad kasutusele Euroopa ühendamise rahastu eDelivery komponendi, lihtsalt ja turvaliselt vahetada teavet isegi siis, kui nende IT-süsteemid on välja töötatud üksteisest sõltumatult. eDelivery mudel on küll väga kasulik, et luua ühendus mitme tagarakendussüsteemiga, kuid selle eri funktsioone saaks ka tsentraliseerida. Seda tehnoloogilist lahendust kasutades peaksid liikmesriigid (ja võimalik, et keskse marsruutimiskomponendi puhul ka komisjon) võtma oma tasandil kasutusele eDelivery digivärava. Nad saavad taaskasutada olemasolevaid võrgusõlmi, mis on välja töötatud teiste teenuste jaoks (see aitab kaasa lahenduse kulutõhususele). Olemas on ühilduv tarkvaralahendus, mille on välja töötanud Euroopa Komisjoni informaatika peadirektoraat ja mille kasutamist pakutakse tasuta Euroopa Liidu tarkvara vaba kasutuse litsentsi (EUPL) alusel. Tavaliselt on siiski vaja teatavat kohandamist ja arendamist. eDelivery mudel kasutab asünkroonset sidet, mis tähendab, et jõudluses esineb vältimatult teatav latentsus (tavaliselt 3–10 sekundit). CEFi elementide puhul on ELi üldine põhimõte, püüelda ELi eri poliitikavaldkondade raames välja töötatavate süsteemid ühtlustamise suunas.

Kui kasutatakse sünkroonset SOAPi, mis võimaldab suhtlust turvalisel kihil, valitakse kõige sagedamini lihtne arhitektuur, mille eesmärk on võimalikult suur jõudlus. RESTfuli arhitektuuristiil esindab SOAPiga võrreldes uuemat lahendust ja välja on kujunemas suund, kus SOAPi protokoll jääb RESTi tehnoloogiale alla. Nii eDelivery kui ka SOAPil või RESTil tuginevate lähenemisviiside puhul põhineb usaldus tavaliselt digitaalsetel sertifikaatidel ning tehakse hulk kontrolle.

Keskmehhanismide tulevase omavahelise ühendamise kohta tuleb märkida, et Euroopa ühendamise rahastu platvormi eDelivery kasutatakse siis, kui tegemist on kahepoolse teabevahetusega liikmesriikide detsentraliseeritud andmebaaside vahel, samas kui süsteemides, kus side toimub üksnes liikmesriigi andmebaasi ja keskse platvormi vahel, piisab SOAPi-põhisest (või RESTfuli-põhisest) liidesest.

4.4. Töö mitmekeelses keskkonnas ja semantiline koostalitusvõime

Kõik hinnatud süsteemid töötavad mitmekeelses keskkonnas, välja arvatud EBOCS, mis töötab praegu kolmes keeles, kuid pikas perspektiivis on eesmärk toimida kõigis keeltes. BRISis toimub transliteratsioon ELi tasandil, kuid IRI, LRI ja EUCARISe puhul liikmesriigi tasandil. Semantilise koostalitusvõime (sõnastike) puhul ei nõua keskmehhanismide tulevane omavaheline ühendamine konkreetset sõnavara, sest minimaalne teave ei koosne liikmesriikide mõistetest, vaid isikuandmetest, sh näiteks nimi, kordumatu tunnus (nt isikukoodid) ja IBAN. Väga oluline on lähtuda kõigis riiklikes süsteemides ühistest põhimõtetest, eeskätt seetõttu, et riiklikud keskmehhanismid ei sisalda teavet ELi ja kolmandate riikide üksuste kohta. Schengeni infosüsteemi transliteratsioonireeglid võiksid olla selles kontekstis kasulik näide.

Euroopa koostalitlusvõime raamistiku (EIF) kohaselt viitab semantiline aspekt andmeelementide tähendusele ja nendevahelistele suhetele. See hõlmab sõnastike ja skeemide koostamist andmevahetuse kirjeldamiseks ning tagab, et kõik suhtlevad pooled mõistavad andmeelemente ühtemoodi.

Pangaregistrite ühendamise süsteemiga hakatakse andmeid vahetama eri andmebaaside vahel, millest igaühel on oma andmemudelid ja semantilised standardid. Vaja on kehtestada ühised semantilised standardid kas süsteemide sees või vastenduskihina liikmesriikide eri standardite vahel. Enne uue semantilise standardi kehtestamist tuleks kaaluda juba olemasolevate standardite taaskasutamist.

Põhisõnastikud (ettevõtte, asukoha, isiku jm kohta), mille on loonud ISA[2] programm, on lihtsustatud, taaskasutatavad ja laiendatavad andmemudelid, mida saab sel eesmärgil kasutada. Baasregistrite, nagu näiteks BRIS, omavahelise ühendamise eri lahendused taaskasutavad juba mõnda standardit (nt ettevõtluse põhisõnastik (*Core Business Vocabulary*)).

5. Edasised sammud

Käesolevas aruandes tuuakse välja mitu elementi, mida pangakontoregistrite ja andmeotsingu süsteemide võimalikul ühendamisel kaaluda, ning näidatakse, et nende kesksete mehhanismide ühendamine on tehniliselt teostatav. Selline süsteem võiks olla detsentraliseeritud süsteem ühise platvormiga ELi tasandil. Kasutada võib tehnoloogiat, mille Euroopa Komisjon on juba analüüsitud mudelite kontekstis välja töötanud.

Viimastel aastatel on eri süsteemid järginud ühiste elementide uuesti kasutamise võimalust. Need elemendid on põhimõtteliselt hästi tuntud standardid ja tehnilised kirjeldused, mida on võimalik kohaldada korduvate probleemide (nt turvalise teabevahetuse) lahendamiseks. Nende elementide järjepidev kasutamine on lähenemisviis, mida toetab komisjoni praegune digitaalpoliitika, mida liikmesriigid Tallinna e-valitsemise deklaratsioonis järgida lubasid[28]. Kui liikmesriikide automatiseeritud keskmehhanismid tulevikus ühendatakse, saaks neidsamu elemente kasutada selleks, et kiirendada ühenduse loomist ja vastavusse viimist asjakohaste ELi määrustega, nagu näiteks eIDAS.

Arvestades, et kesksete mehhanismide omavaheline ELi-ülene ühendamine kiirendaks juurdepääsu finantsteabele ja hõlbustaks pädevate asutuste piiriülest koostööd, kavatseb komisjon jätkata konsulteerimist sidusrühmade, valitsuste, aga ka rahapesu andmebüroode, õiguskaitseasutuste ja kriminaaltulu jälitamise talitustega kui võimaliku ühendsüsteemi potentsiaalsete lõppkasutajatega.

[28]Kõik Euroopa Liidu liikmesriigid ja EFTA riigid allkirjastasid e-valitsemise deklaratsiooni Tallinnas 6. oktoobril 2017. Deklaratsiooni tekst on kättesaadav aadressil http://ec.europa.eu/newsroom/document.cfm?doc_id=47559.