TALLINNA TEHNIKAÜLIKOOL

Sotsiaalteaduskond

Õiguse instituut

Aet Veges

Andmekaitse mobiilse tervishoiu puhul

Bakalaureusetöö

Juhendaja: Kari Käsper, MA

Tallinn 2017

Deklareerin, et käesolev bakalaureusetöö,

mis on minu iseseisva töö tulemus,

on esitatud Tallinna Tehnikaülikooli

bakalaureusekraadi taotlemiseks ja selle alusel

ei ole varem taotletud akadeemilist kraadi.

Üliõpilane Aet Veges

“ ….. “ …… 2017

Töö vastab kehtivatele nõuetele

Juhendaja Käri Käsper, MA

“ ..... “ 2017

Kaitsmisele lubatud “ ..… “ 2017

Avaliku halduse magistritööde kaitsmiskomisjoni esimees

Sisukord

Sissejuhatus

Nutitelefonide, tahvelarvutide ning teiste andmetöötluse ja infokogumisega tegelevate „tarkade“ seadmete kasutamine on infoühiskonna arenguga muutunud tavapäraseks. Teatud mõttes on selliseid arukad seadmeid inimese elu-olu arhiiviks . Telefoni muudab nutikaks arvutipõhine ülesehitus. Seadme keskmes on operatsioonisüsteem, mida saab võtta seadme ajuna ning mille eesmärgiks on pakkuda interneti keskseid teenuseid. Erinevate tarkvara aplikatsioonide kasutamine võimaldab osaleda kogukonna elus ja määrata ning reguleerida sündmusi. Kõik aplikatsioonid ehk äpid koguvad ja töötlevad inimesega seotud informatsiooni.

Autori bakalaureusetöö keskendub mobiilse tervishoiuga (edaspidi m-tervishoid) seotud äppide alagrupile. Tegemist on rakendustega, mida on võimalik kasutada kas meditsiinilistel või tervisega seotud eesmärkidel. Need äpid töötlevad inimeste tervisega seotud andmeid ehk delikaatseid isikuandmeid, andmeid mis on oluliselt rangema kaitse all oma tundliku iseloomu tõttu. Oma olemuselt on m-tervishoiu sisu äärmiselt varieeruv, mõiste alla lähevad nii lihtsakoelised rakendused, mille eesmärgiks on kokku arvutada kasutaja poolt astutud sammud päeva jooksul, kuid on olemas ka äppe, mis suudavad andmeid kombineerides kasutajale diagnoosi anda või näiteks seadme keskseid sensoreid kasutades meenutada alzhaimeri haigetele nende asukohta.

Statistika kohaselt omab üle pool Eesti elanikkonnast nutitelefoni. Igapäevaselt lisatakse juurde mobiilsete rakenduste poodi üle 1000 uue rakenduse.[1] Ning keskmine nutiseadme kasutaja tõmbab endale alla umbes 37 rakendust ning ühe rakenduse taga võib olla üle miljoni inimese.[2]

Tegu on helikiirusel areneva sektoriga ning umbkaudu on hetkel turul olemas üle 100 000 erineva tervisega seonduva äppi.[3] Maailma Tervishoiu Organisatsiooni andmete kohaselt on

[1] EMOR. Nutiseadmete kasutajate turvateadlikkuse ja turvalise käitumise uuring, 2014. https://www.ria.ee/public/Programm/Nutiseadmete_kasutajate_turvateadlikkuse_ja_turvalise_kaitumise_uuring_ARUANNE_2014_LUHI2.pdf (10.12.2016)

[2] Artikkli 29 alusel asutatud andmekaitse töörühm. Arvamus 02/2013 nutiseadmete rakenduste kohta, 2013. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_et.pdf (10.11.2016)

[3] Research2Guidance. Mobile health app market report 2013–2017: The commercialization of mHealth. Research2Guidance, 2013.

just Euroopas asetsevad riigid kõige aktiivsemateks tervishoiu rakenduste kasutajateks.[4] Tegemist on valdkonnaga, mis võib kaasa endaga tuua tervishoiu sektori täieliku muutuse. Enam ei mängi kasutaja geograafiline asukoht mingisugust rolli ning erinevaid terviseandmeid kombineerides on võimalik teadlastel teha uusi avastusi haiguste vallas, samuti on tegemist efektiivse vahendiga, mis annab kasutajale võimaluse oma tervisel rohkem silma peal hoida. Kuid andmekaitse seisukoha pealt on tegemist problemaatilise uuendusega, millele keskendub ka autori töö.

Info- ja kommunikatsiooni tehnoloogia (IKT) ning andmekaitse on terminid, mis on üksteisest lahutamatud. IKT arengu üheks kriteeriumiks on andmekaitse. IKT kiire areng 50ne aasta jooksul on täielikult reformeerinud privaatsuse mõiste tuues endaga kaasa küsimuse, kas privaatsust veel üleüldse eksisteerib. Seda seisukohta toetab ka Euroopa Liidu Põhiõiguste ameti pool läbi viidud uuring, kus selgus, et enamjaolt on andmekaitsereeglite rikkumise seotud interneti kasutamisega.[5] Kui võrrelda aplikatsioone tavapäraste veebilehitsejatega, siis selgub, et äppidel on tunduvalt suurem võimalus pääseda ligi erinevatele andmetele.[6] Juba läbi asukoha määramise või fotoalbumile ligipääsu saades on võimalik koguda suurtes kogustes äärmiselt delikaatset informatsiooni. Kõige suurem riskifaktor seisneb toimingute läbipaistmatuses ehk siis kogutud teavet on võimalik kasutada edasi sellisel moel, millest kasutajal aimugi ei ole või mida ta ei soovi. Millest tulenevalt ei pruugi lõppkasutaja oma kuvandi üle omada mingit kontrolli. Globaliseerinud ühiskond on endaga kaasa toonud selle, et informatsioon on muutunud digimaailma naftaks.

---

http://www.researchandmarkets.com/reports/2497392/mobile_health_app_market_report_20132017_the (03.11.2016)

[4] World Health Organization. mHealth - New horizons for health through mobile technologies, 2011. http://www.who.int/goe/publications/goe_mhealth_web.pdf (12.10.2016)

[5]Euroopa Liidu Põhiõiguste Amet. Juurdepääs andmekaitse õiguskaitsevahenditele Euroopa Liidu liikmesriikides. Kokkuvõte, 2013. http://bookshop.europa.eu/et/juurdepaeaes-andmekaitseiguskaitsevahenditele-euroopa-liidu-liikmesriikides-pbTK0113752/downloads/TK-01-13-752
ETC/TK0113752ETC_002.pdf?FileName=TK0113752ETC_002.pdf&SKU=TK0113752ETC_PDF&CatalogueNu
mber=TK-01-13-752-ET-C (12.10.2016)

[6]Artikkli 29 alusel asutatud andmekaitse töörühm. Arvamus 02/2013 nutiseadmete rakenduste kohta,2013 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_et.pdf (10.11.2016)

Infoühiskonna areng ei ole seotud ainult tehniliste näitajatega, vaid seda saab seostada tihedalt põhiõiguste ja demokraatia endaga.[7] Õigus privaatsusele ning sellelt tulenevalt andmekaitse on Euroopa Liidu üheks põhiõiguseks, mis väärib kaitset kõikide suhtes. [8] Õiguslikud regulatsioonid ei pruugi aga piisavalt kiiresti ajaga kaasa käia, mis tähendab seda, et seadusloome ei ole suuteline arvestama tehnoloogilise reaalsusega, mis muudab õigusnormid ebaefektiivseteks õõnestades omakorda õiguskindlust. Kuna IKT ja andmekaitse on niivõrd tihedalt omavahel seotud on seadusloojal raske ülesanne leida harmoonia tugeva andmekaitselise raamistiku ning tehnoloogilise innovatsiooni vahel. Eelnevad kogemused on näidanud seda, kui oluline on leida tasakaal turvalise keskkonna pakkumise ning liiga piiravate turvanõuete vahel, sest üks võib pärssida teist.

Bakalaureusetöö eesmärgiks on analüüsida Euroopa Liidu andmekaitseõiguse sobivust ning kohaldatavust mobiilse tervishoiu valdkonnale. Töö hüpoteesiks on seatud see, et olemasolev andmekaitse õiguslik raamistik ei ole piisav selleks, et tagada terviseandmete efektiivset kaitset m-tervishoiu valdkonnas.

Käesolev töö on üles ehitatud baseerudes Euroopa Liidu andmekaitseõigusel ning selle erinevatel tahkudel. Õigusnormide sisustamisel on kasutatud erinevaid ekspertide arvamusi alates Artikkel 29 alusel loodud andmekaitse rühmast, Euroopa Andmekaitse Inspektori kuni Eesti Andmekaitse Inspektsioonini. Kuigi autorit saab kritiseerida selletõttu, et enamjaolt on kasutatud elektroonilisi allikaid on selline valik tehtud teema uudsuse tõttu, mille pärast paberkandjal teema kohast kirjandust väga ei eksisteeri. Enamjaolt on tegemist välismaise materjaliga, sest Eesti teaduskirjanduses pole valdkonda hetkel autorile teadaolevalt veel uuritud, sellest olenemata on kasutatud mõningaid teemaga kaudselt seotud olevaid Juridica artikleid, samuti varasemaid analoogse sisuga töid. Autori töös on ennekõike kasutatud analüütilist meetodit selleks, et vastata teesis püstitatud küsimusele.

Bakalaureusetöö jaguneb kolmeks peatükiks. Esimene peatükk on ennekõike illustreeriva iseloomuga. Antakse ülevaade autori pool nii olemasolevale õiguslikule raamistikule, kui ka kesksetele mõistetele selleks, et teemat avada. Peatükis seletatakse lahti sellised mõisted nagu privaatsus, isikuandmed ning terviseandmed.

[7]Tupay, P-K., Mikiver, M. E-riik ja põhiõigused. Juridica, 2015, 3, lk 163-176.
[8]De Filippi, P., Belli, L. Law of the Cloud v Law of the Land: Challenges and Opportunities for Innovation. – European Journal of Law and Technology, 2012, 3 (2), lk 2.

Teises peatükis vaatleb autor, mida täpsemalt tähendab terviseandmete töötlus m-tervise kontekstis. Kuna terviseandmete parameeter on võrdlemisi lai on tähtis teha vahet heaolu teabel, millel pole mingit kaalu ning terviseandmetel. Keskendatud on samuti tehnoloogilistele trendidele nagu suurandmestik, andmekaeve ning pilvetehnoloogia. Tegemist on hilisema andmetöötluse vormiga, mis on senisest suurema mahuga ning ülimalt kiire. Autor analüüsib, kas ning kuidas andmekaitse printsiipe on vastavalt võimalik kohandada.

Kolmanda peatüki raames vastatakse küsimusele, kas olemasolevat õigusliku raamistiku saab efektiivselt kohaldada mobiilse tervishoiu maailmas. Autor vastab töö alguses püstitatud küsimusele analüüsides vastavaid sätteid põhjalikumalt ning tehes vastavalt omad järeldused ning ettepanekud.

Teema valiku puhul innustas autori ennekõike see, et Eestis pole teadaolevalt mobiilseid rakendusi, veel vähem m-tervishoidu akadeemiliselt uuritud. Eesti vaatepunktist on tähtis teema vaatlus ka selletõttu, et ennekõike oleme tuntud maailmas, kui e-Estonia, mis on riigi suurimaks monopoliks. Hetkel on Euroopa Komisjoni ja OECD poolt avaldatud aruande poolt, Eesti esirinnas e-teenuste valdkonnas, tähtis on see, et jääksime juhtivale kohale.[9]

[9]PwC Luxembourg. European Hospital Survey: Benchmarking Deployment of eHealth Services (2012–2013), 2014. http://ipts.jrc.ec.europa.eu/publications/pub.cfm?id=7060 (21.10.2016)

1. Kesksed mõisted ning olemasolev õiguslik raamistik

1.1 Õigus privaatsusele, kui andmekaitse alus

Privaatuse ning andmekaitse mõisted on üksteisega tihedas suhtes, sest üks ei saa eksisteerida ilma teiseta. Privaatsust saab mõista kui isiku võimet eraldada mina pilti ühiskonnast, millest tulenevalt saab järeldada ning väita, et andmekaitse oma olemuselt toetab ning kinnistab seda võimalust. Tegemist on universaalsete ideedega, millel on olemas äärmiselt tugevad eetilised väljundid.[10]Õigust eraelule saab pidada üheks demokraatliku õigusriigi alustalaks, sest oma olemuselt puudutab see igaüht. Hea valitsemiskorraga riigis on võime hoida eraldatust väga austatud ning sellest tulenevalt ka hinnatud. Fakt on see, et jälgimise all muudab inimene oma käitumist kardinaalselt, mille tulemusel võib väita, et privaatsuse olemasolu ning kaitse on tähtsad selleks, et eksisteeriks normaalne ühiskond.

Globaalses maailmas on üsna tavaline see, et kõike enda kohta jagatakse terve maailmaga. See, mis oli enne vaid valitsuse privileegiks on nüüd muutunud üksikisiku võimaluseks. Tsiteerides Sun Microsystem'i endist juhti Scott McNealyt:"You have zero privacy anyway. Get over it" või megakompanii Facebooki asutajat Mark Zuckerbergi: „Privacy is no longer a social norm". Autor on siiski seisukohal, et tavakasutaja pole teadlik ohtudest, mille tõttu on seadusloojal ülesanne luua tugevad kriteeriumid ning normid millest juhinduda. Isiku võime ja võimalus hoida enda kohta käivat informatsiooni saladuses on äärmiselt oluline selletõttu, et see annab võimaluse arendada individuaalsust, mis ei ole dikteeritud ülejäänud maailmast tulenevalt.[11]

Esmakordselt tunnustati ja toonitati isikuandmete ja privaatsuse kaitse tähtsust juba aastal 1890. Samuel D.Warreni ja Louis D. Brandeisi artiklis "The Right to Privacy", mida saab pidada üheks kõige mõjukamaks esseeks Ameerika Ühendriikide õiguskirjanduses. Üle saja aastases artiklis on välja toodud seos tehnoloogia arengu ning privaatsuse vahel (kuigi tol ajal mõeldi selle all ajakirjanduse levikut), mis on siiamaani relevantne. Kuigi isikuandmete kaitse

[10]Hustinix, P. EU Data Protection Law - Current State and Future Perspectives, 2013 http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/Hustingx.pdf (07.01.2017)

[11]Euroopa Inimõiguste Kohus (EIK) on 24. juuni 2004. a lahendis Von Hannover vs. Saksamaa märkinud, et eraelu kontseptsioon laieneb ka identiteedile

selles vormis nagu meie seda tunneme saab pidada suhteliselt verinooreks, muutudes päevakorraliseks alles 1970nendatel seoses andmetöötlusvahendite massilisele arengule.

Moodsale Andmekaitsele pandi alus ÜRO Inimõiguste Deklaratsiooniga, mille artikkel 12 sätestab selle, et kellegi isikliku või perekonnaellu ei või meelevaldselt segada. Igal inimesel on õigus seaduse kaitsele selliste vahelesegamiste eest.[12] Deklaratsiooni täiendas kaks aastat hiljem vastu võetud Inimõiguste ja Põhivabaduste Konventsioon (edasipidiselt EIÕK), mis on siiamaani Euroopa Nõukogu kõige tähtsamaks dokumendiks. Konventsiooni artiklis 8 on samamoodi välja toodud eralu puutumatuse mõiste ning selle kaitse. Kuigi terminitel eraning pereelu ei ole otsest seost andmekaitsega on Euroopa Inimõiguste Kohus (EIK) siiski läbi erinevate kohtulahendite jõudnud otsusele, et seda on otseselt võimalik tuletada artikkel 8-st, mis sätestab andmekaitsele minimaalsed reeglid järgimiseks. Liit on vastavalt sellele avaldanud seisukohta, et eralu puutumatust saab võrdsustada andmekaitsega.[13] EIK-i lahendid on mänginud suurt rolli privaatsusõiguse sisustamisel, andes uudseid tähendusi ning muutes artikli „elavaks" rakenduseks.[14]

Kui vaadelda andmekaitse norme rahvusvahelisel tasandil, siis on näha, et hetkel on kokku lepitud vaid üldprintsiipides. Kuigi EIÕK on üheks kõige olulisemaks õigusnormiks liidu tasandil peab arvestama sellega, et tegemist on vana dokumendiga, millest tulenevalt ei pruugi see olla kõige proaktiivsemaks lahenduseks. Mille tõttu on artiklit ka kritiseeriud. Kui analüüsida sõna eraelu iseseisvalt, siis on näha, et tegemist in vägagi abstraktse mõistega, kust ennekõike saab välja lugeda vaid ametivõimude sekkumise mitte lubatavust, mida peeti artikli loomise ajal esmaselt silmas.[15] Vaatamata sellele on tegemist primaarse andmekaitse alase normiga. [16]Euroopa Liit ei ole EIÕK-iga küll õiguslikult seotud (kuigi kõik liikmesriigid on konventsiooni ratifitseerinud), kuid see on olnud suureks eeskujuks hilisemate õiguste kujundamisel.

[12] United Nations. The Universal Declaration of Human Rights, 10.12.1948 § 12.
[13]Ilus, T. Andmesubjekti osaluse põhimõte Euroopa Nõukogu konventsioonide ning Euroopa Inimõiguste kohtu lahendite valguses. Juridica, 2005, 8, lk 520.
[14]Letsas, G. The ECHR as a living instrument: its meaning and legitimacy. In Constituting Europe. The European Court of Human Rights in a National, European and Global Context. Cambridge University Press: Cambridge 2013, lk 109-111.
[15]De Hert, P., Gutwirth, S. Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action. Reinventing Data Protection. Dordrecht: Springer Science 2009, lk 5.
[16]Fink, U. Protection of privacy in the EU, individual rights and legal instruments. in Emerging Challenges in Privacy Law. Comparative perspectives. Cambridge: Cambridge University Press 2013, lk 75.

Euroopa aluslepingusse polnud algselt sisse toodud fundamentaalseid inimõigusi. Selleks, et üksikisikuid kaitsta toodi põhiõigused Euroopa õiguse üldpõhimõtetesse alles siis, kui kohtutel suurenes oluliselt vajadus mõista õigust küsimustes, mis puudutasid liidu raames inimõiguste rikkumisi. Uue Euroopa nägemus manifesteerus Euroopa Liidu Põhiõiguste Hartaga. Algselt oli tegemist vaid poliitilise dokumendiga, kuid seoses Lissaboni lepinguga muutus see kõikidele liikmesriikidele õiguslikult siduvaks.[17] Tänasel päeval loetakse Hartat Euroopa Liidu Põhiseaduse lepingu teiseks osaks.[18]

Harta artikkel 7 on samasuguse sõnastusega, kui talle eelnenud EIÕK-i artikkel 8. Kuid harta artikli 8-ga anti esmakordselt isikuandmete kaitele põhiõiguslik tunnustus. Eraldi õigusena toodi välja nii andmekaitse, kui ka andmekaitse standardid, mida tuleb töötlusel järgida ning millest on juhindunud uus Isikuandmete Kaitse Üldmäärus (GDPR) ning korduvalt ka Euroopa Kohus. Harta artikkel 8 lõige 1 sätestab, et andmeid tuleb töödelda asjakohaselt ning kindlaksmääratud eesmärkidel ja asjaomase isiku nõusolekul või muul seaduses ettenähtud õiguslikul alusel. Igaühel on õigus tutvuda tema kohta kogutud andmetega ja nõuda nende parandamist.

Andmekaitse tõstmine põhiõiguslikule tasandile tõi endaga kaasa konstitutsioonilisel tasandil toimuva kvalitatiivse muutuse.[19]Põhiõiguse staatuse andmisega tasakaalustati suhteid andmesubjekti ning ettevõtjate õiguste vahel.[20] Artiklit on jällegi kritiseeritud selletõttu, et mõisted eraelu puutumatus ning isikuandmed on omavahel tihedalt soetud.[21] Autori arvates on selline seisukoht siiski küsitav, nõustudes endise Euroopa Andmekaitse Inspektori Peter Hustinixiga, kes on öelnud, et andmekaitseõiguse kaitseala on oluliselt laiem selletõttu, et see omab endas teisi põhiõigusi.[22] Autor on seisukohal, et mõisteid ei saa mõista, kui üksteise sünonüüme, vaid peaks vaatama koostoimes ning teineteist täiendavalt. Vaadelda saab ka

[17]Commission of the European Communities. European Comission report. First report on the implementation of the Data Protection Directive (95/46/EC), 2003. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2003:0265:FIN:EN:PDF (03.12.2016)
[18]Laffranque,J. Eesti põhiseaduse ja Euroopa õiguse kooselu. Juridica, 2003,3, lk 180-190.
[19]European Commission. EU Charter of Fundamental Rights. (2000/C 364/01) § 8
[20]De Hert, P., Gutwirth, S. Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action. Reinventing Data Protection. Dordrecht,Springer Science 2009, lk 10.
[21] Lynskey, O. Deconstruction Data Protection: The „Added-Value“ of a Right to Data Protection in the EU Legal Order.- International & Comparative Law Quarterly ,2014, 3 (63), lk 570 .
[22]Hustinx, P. EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation, 2014. http://www.statewatch.org/news/2014/sep/eu-2014-09-edps-data-protection-article.pdf (13.11.2016)

Euroopa Liidu toimimise lepingu artiklit 16, millest tulenevalt lasub seadusandjal kohustus tagada efektiivne kaitse andmekaitse vallas, ning mille alusel võeti vastu ka uus GDPR.

1.2 Isikuandmete ning terviseandmete mõisted

Nagu autor on eelnevalt välja toonud on andmekaitse kõige kesksemaks mõisteks isikuandmed, millele on üles ehitatud kogu õigus. Isikuandmeteks on igasugune teave tuvastatud või tuvastatava füüsilise isiku kohta. Eelkõige selliste identifitseerimistunnuse põhjal nagu nimi, isikukood, asukohateave, võrguidentifikaator või selle füüsilise isiku ühe või mitme füüsilise, füsioloogilise, geneetilise, vaimse, majandusliku, kultuurilise või sotsiaalse tunnuse põhjal.[23] Kui vaadelda sõnu igasugune teave on näha, et tegemist on väga üldise mõistega.

GDPR-is seadusandja poolt antud definitsioon on väga lai põhjusega. Artikli 29 alusel loodud töögrupp (töögrupp) põhjendas seda valikut oma arvamuse avalduses sellega, et potentsiaalselt võib ükskõik milline informatsioon olla personaalne, mille tõttu on oluline, et definitsioonis on olemas sõna „igasugune".[24]Samuti andmed, millel esmapilgul ei pruugi olla mingisugust väärtust võivad aja jooksul pärast erinevate rakenduste kasutust muutuda isikustatud teabeks.[25]Abstaktne lähenemisviis on valitud seetõttu, et mõistet oleks võimalik kohaldada igas olukorras ning erinevate arengusuundade suhtes (arvestades IKT kiiret arengu võimalust).

Kuigi mõiste on avar, ei ole see siiski oma olemuselt täiesti piiramatu. Õigusnormi tuleb analüüsida olukorras, kus üksikisiku õigused on sattunud ohtu. Töögrupp on kommenteerinud olukorda nii, et andmekaitse alased nõuded ei tohiks olla üleliia laialivalguvad kuna see külvab segadust, kuid samuti on oluline see, et definitsiooni ei tohiks mõistmatult kitsamaks

[23]European Comission. Regulation 2016/679 of 27.aprill 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, OJ L 119, 4.05.2016 § 4.
[24]Artikkel 29 alusel asutatud andmekaitse töörühm. Arvamus 4/2007 isikuandmete mõiste kohta, 2007. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_et.pdf (04.04.2017).
[25]Van der Sloot, B. Do data protection rules protect the individual and should they? An assessment of the proposed General Data Protection Regulation.-International Data Privacy Law, 2014, 4 (4), lk 309.

teha.[26]Selleks, et jõuda järeldusele, mis täpselt konstitueerib personaalse teabe alla tuleks GDPR-is välja toodud elemente põhjalikult analüüsima selleks, et leida vastavused olemasoleva teabega.

Isikuandmeid saab jagada omakorda eriliikideks, mida nimetatakse delikaatseteks andmeteks ning mis on olulisemalt rangema kaitse all. Delikaatsete andmete alla lähevad GDPR-i artikkel 9 kohaselt kõik andmed, mis kirjeldavad isiku usulisi, poliitilisi ja maailmavaatelisi veendumusi, etnilist ja rassilist kuuluvust, terviseseisundit, puuet, pärilikkust, ametiühingu liikmelisust ja seksuaalelu.[27] Seadusandja on kommenteerinud karmimat lähenemist sellega, et kui kasutada delikaatseid andmeid ära valedel eesmärkidel, siis võib see endaga kaasa tuua olulisemalt suurema kahju üksikisikute põhiõigustele.[28]

Bakalaureusetöö keskseks teemaks on ennekõike terviseandmed. Kui varasemalt oli kohtu otsustada, mis täpsemalt läheb terviseandmete kategooria alla on esmakordselt mõistele antud seaduses definitsioon. Üldmääruse artikkel 4-ga on sätestatud, et terviseandmed on füüsilise isiku füüsilise ja vaimse tervisega seotud isikuandmed, sealhulgas temale tervishoiuteenuste osutamist käsitlevad andmed, mis annavad teavet tema tervisliku seisundi kohta. Töögrupp on avaldanud arvamust, et tegemist on ühe kõige kompleksemaks andmeliigiks oma ülimalt tundliku natuuri tõttu.[29]

Kui võtta lause jällegi osadeks, siis saab järeldada sõnade füüsilise ja vaimse tervisega seotud tähendusest, et parameeter on jällegi ääretult lai. Näiteks läheb terviseandmete kategooria alla fakt, et isik kannab prille või kontaktläätsesi, andmed intellektuaalse ning emotsionaalse

[26]Artikkel 29 alusel asutatud andmekaitse töörühm. Arvamus 4/2007 isikuandmete mõiste kohta, 2007 (04.04.2017)
[27]European Comission. Regulation 2016/679 of 27.aprill 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, OJ L 119, 4.05.2016 § 9.
[28]Artikkel 29 alusel asutatud andmekaitse töörühm. Advice Paper on Special Categories of Data (sensitive data), 2000. http://www.europarl.europa.eu/charter/pdf/text_en.pdf
http://ec.europa.eu/justice/data-protection/article
29/documentation/otherdocument/files/2011/2011_04_20_letter_artwp_mme_le_bail_directive_9546ec_annex1_en.pdf
(20.02.2016)
[29]Artikkel 29 alusel asutatud andmekaitse töörühm. Advice Paper on Special Categories of Data (sensitive data), 2000. http://www.europarl.europa.eu/charter/pdf/text_en.pdf
http://ec.europa.eu/justice/data-protection/article
29/documentation/otherdocument/files/2011/2011_04_20_letter_artwp_mme_le_bail_directive_9546ec_annex1_en.pdf
(20.02.2017)

taseme kohta, kas isik tarbib alkohoolseid jooke või suitsetab, allergiad *etc*. Isegi teave indiviidi liikmelisuse kohta, kui tegemist on näiteks kas kaalulangetajate või anonüümsete alkohoolikute grupeeringuga, sest tegu on tervisega seonduva objektiiviga.

1.3 Isikuandmete Kaitse Üldmäärus

Euroopa Komisjon tõi välja oma teatises, et Euroopa peab võtma kursi ulatuslikumale ning terviklikumale lähenemisele, mida rakendades oleks võimalik tagada andmekaitse austamine põhiõigusena.[30]Kuigi eelnenud direktiivi poolt paika pandud raamistiku põhitõed on siiamaani ajakohased tekkis ajapikku vajadus uue regulatsiooni järgi.[31] Seda toetas fakt, et Euroopa Komisjoni poolt läbi viidud Andmekaitsedirektiivi rakendamise hindamine näitas seda, et direktiivi ülevõtmisel liikmesriikidele jäetud vormi ja meetodite valik ning riigiti erinevad ühiskondlikud ja õiguslikud arusaamad on endaga kaasa toonud direktiivi oluliselt erineva käsitluse, mille tõttu on tekkinud fragmentatsiooni tõttu oluliselt suurem administatiivne koorem.[32]Sellest tulenevalt on uus regulatsioon kirja pandud üldkohaldatava määrusena, mis on terviklikult liikmesriikides siduv, mis ideaali kohaselt peaks elimineerima tekkinud killustatuse.[33]Vaadates kohtulahendeid selgub, et EIK on juba varasemalt toonitanud andmekaitsereformi vajadust põhjendades seda sellega, et vajalik on detailsemate reeglite olemasolu, mis oleks samaaegselt kooskõlas tehnoloogiliste asjaoludega.[34]

[30]Euroopa Liidu Põhiõiguste Amet. Twelve operational fundamental rights considerations for law enforcement when processing Passenger Name Record (PNR) data, 2014. https://www.google.ee/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwitrO2N6s_TAhWjKJoKHUrvA5IQFgglMAA&url=https%3A%2F%2Ffra.europa.eu%2Fsites%2Fdefault%2Ffiles%2Ffra-2014-fundamental-rights-considerations-pnr-data-en.pdf&usg=AFQjCNFrhjNS8_oxAv0aGHBl2eGCSFD6VQ&sig2=dFJT8JP68nVXHvPCX_nlFw (23.01.2017)

[31]Euroopa Komisjon. Komisjoni teatis Euroopa Parlamendile,Nõukogule, Majandus- ja Sotsiaalkomiteele ning Regiooni Komiteele. Terviklik lähenemisviis isikuandmete kaitsele Euroopa Liidus, 2010 http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_et.pdf (23.01.2017)

[32]European Commission. Commission Staff Working Paper. Impact Assesment, 2012. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=SEC:2012:0072:FIN:EN:PDF (17.12.2016)

[33]Euroopa Komisjon. Kuidas kohandatakse ELi reformiga andmekaitse-eeskirju uue tehnoloogilise arenguga?, 2016 http://ec.europa.eu/newsroom/document.cfm?doc_id=41579 (17.12.2016)

[34] EIK 25.03.1998, 13/1997/797/1000, Kopp v Šveits, p 72.

GDPR-i saab ennekõike võtta, kui eelnenud direktiivi pikendust, sest kontseptsioon ning kesksed mõisted on jäänud muutumatuks. Määrus kätkeb endas varasemast tugevamat raamistikku, mille läbi oleks tagatud nii üksikisikute senisest tugevam ning parem kaitse, kuid samas oleks digitaalsel majandusel olemas võimalus areneda täisvõimsusel edasi kogu siseturu ulatuses.

Uus määrus lähtub põhimõttest, et isikuandmete töötlus peaks ennekõike teenima inimest ennast. Läbivaks teemaks on andmesubjektile anda täielik võim enda kohta käiva informatsiooni üle, mida on kinnistatud täiesti uute printsiipide vastu võtmisega.[35]

Kõige olulisemaks elemendiks on andmetöötlus. Tegemist on nii juurdepääsu võimaldamisega, kui ka andmete edastamisega.[36] Seoses andmetöötlusega peab lähtuma kolmest printsiibist, mis on omavahel tihedalt suhestunud – seaduslikkus, õiglus ning läbipaistvus.

Selleks, et terviseandmete töötlemine oleks seaduslik, õiglane ja läbipaistev äppides, peab andmesubjekt andma oma selgesõnalise ning üheselt mõistetava nõusoleku. Teatud juhtudel võib sellest nõudest kõrvale kalduda (Art 9, lg 2 h) , kui töötlus on vajalik meditsiinilistel põhjustel, töötaja töövõime hindamisel, diagnoosimiseks, kui m-tervishoid selle kategooria alla ei hetkel veel ei lähe (kuigi juttu on tehtud statistiliste uuringute lubatavuses võimalusest selleks, et parandada tervisekvaliteeti).

Nõusolek tuleb andmesubjektil saada enne andmetöötluse protsessi algamist, millega antakse andmesubjektile mõista, et tegemist on tundlikute andmete töötlusega. Nõusoleku selgus kätkeb endas põhimõtet, et kasutaja peab teadlik olema, milline on rakenduse loomus, miks seda kasutatakse, kaua protsess kestab ning millised riskitegurid kaasnevad.[37]Andmesubjektile suunatud informatsioon peab olema võimalikult lihtne ning arusaadav ka inimese jaoks kes ei tunne spetsiifilist terminoloogiat.[38]

---

[35]Euroopa Komisjoni teatis. Terviklik lähenemine isikuandmete kaitsele Euroopa Liidus, 2010. http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_et.pdf (23.01.2017)
[36]Matjus, M., Haamer, M. E-tervis. Millistel tingimustel võib edastada patsiendi terviseandmeid Euroopa Liidu teise liikmesriiki?Juridica, 5, 2014, lk 361-373.
[37]Wetherall, D., Choffnes, D., Greenstein, B., Han, S., Hornyack ,P., J, Jung., Schecter, S., Wang, X. Privacy Revelations for Web and Mobile Apps. University of Washington: Intel Labs , 2011, lk 1.
[38]Robinson, N., Graux, H., Botterman, M., Valeri, L. Review of the European Data Protection Directive. Cambridge: RAND 2009, lk 28.

Läbipaistvuse põhimõte on üheks eelduseks sellele, et subjektil on kontroll enda kohta käiva teabe üle, mida on rõhutanud ka töögrupp.[39] Õiguse rakendamine on raskendatud olukorras, kus andmesubjekt pole teadlik, kuidas ning kes tema kohta käivaid andmeid kogub. Mille tõttu on on oluline üheselt mõistetava privaatsuspoliitika olemasolu, kust üheaegselt saadakse kätte andmesubjekti nõusolek ning seletatakse andmesubjektile arusaadavas vormis tingimusi.

Selleks, et suurendada subjekti õigusi on lisatud määrusesse täiendav peatükk töötlejate vastutuse kohta, mis peaks suurendama õigusselgust ning olema selgitav digitaalses kontekstis, kus töötlejate ring on olulisemalt suurem. Aja jooksul on hajunud piirid traditsioonilise andmetöötleja vahel, seda seoses suurandmestiku ning pilvetehnoloogia kasutusele võtuga. Üldmäärusega sätestatakse kaasvastutavate töötlejate vastutus, määratud on täiendavalt ära ka volitatud töötajale kohustused. Vastutaval töötlejal lasub seadusest tulenev kohustus tagada see, et andmetöötlus oleks kooskõlas üldmäärusega. Autor on arvamusel, et uue peatüki näol on tegemist positiivse ning õnnestunud lahendusega, sest eelnevalt oli teemat puudutatud äärmiselt lühidalt.[40] Lisakohustuste otsene seadusest tulenev olemasolu muudab õiguse rakendamise oluliselt efektiivsemaks

Andmesubjekti õiguste suurendamise ideest subjektil uudne võimalus nõuda oma andmete kustutamist, mis kinnitab omakorda põhimõtet, et subjektil on ainuõigus enda käiva kohta.[41]Õigus tähendab seda, et subjektil on võimalus teenuse pakkujalt nõuda kätte enda kohta käivat ning otsustada, mida selle teabega edasi teha.. Autori arvates võib praktikas olla see siiski raskendatud, mille tõttu ei ole tegemist kõige õnnestunuma printsiibiga, sest põhimõte ei ole vastavus tehnoloogilise reaalsusega.[42] Kõik, mis netiavarustesse paisatakse võib jääda sinna igaveseks, sest andmeid töödeldakse edasi suurejooneliselt ning kiiresti, mis tähendab seda, et esialgne andmetöötleja ei pruugi omada ülevaadet kolmandatest osapooltest.

[39]Artikli 29 alusel asutatud andmekaitse töörühm. Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data. The future of privacy,2009. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2009/wp168_en.pdf (13.02.2017)
[40]Hon, W.K,. Kosta, E., Millard, C., Stefanatou, D. Cloud Accountability: The Likely Impact of the Proposed EU Data Protection Regulation. Queen Mary University of London, School of law,London 2014, lk 14 - 15.
[41]Reding, V. The EU Data Protection Reform 2012: Safeguarding Privacy in a Connected World. Speech, 2012. http://europa.eu/rapid/press-release_SPEECH-11-183_en.htm (04.02.2017)
[42]Zanfir, G. The right to Data portability in the context of the EU data protection reform. -International Data , Privacy Law, 2012, 2 (3), lk 156.

Kuna õigus kustutusele on vastandlik sõnavabaduse põhimõttele tekib küsimus, millisel juhul on tegu tsenseerimisega.

Autori arvates on kõige olulisemaks ning õnnestunumaks lahenduseks arvestades m-tervishoiu valdkonda artikli 25 sisse toomine ehk siis andmekaitse vaikimisi ja lõimimise printsiibi tutvustus. Põhimõte on üles ehitatud arvestades seda, et privaatsust ei ole võimalik tagada alati tänu õigusnormide olemasolule, vaid peab tulenema vaikimisi organisatsioonilisest töökorraldusest.[43]

Selleks, et tagada isikute õigus ning vabadusi senisest efektiivsemalt tuleb vastu võtta vastavaid korralduslikke ning tehnilisi meetmeid. Ehk privaatsuse tahku peab inkorporeerima toote või teenuse disaini juba loomeprotsessis. Kuigi üldmääruses pole välja toodud, kuidas põhimõtet rakendada ei ole tegemist tundmatute mõistega.[44]Selleks, et põhimõtet rakendada saab juhinduda varasemalt tuntud 7-st printsiibist:[45]

1) Meetmed peavad olema ennetavad ja ärahoidvad. Ehk siis eraelu riive oht tuleks elimineerida enne selle toimumist.
2) Andmekaitse võtmine püsiseisundina ehk isikuandmete kaitse võiks toimida süsteemis automaatselt.
3) Andmekaitsesse suhtumine, kui süsteemi ühesse ülesehituse osasse, ilma funktsionaalsuse kaota.
4) Täielik otstarbekus. Arvesse on võetud mõlema poole huvisid, valikud on otstarbekad nii andmesubjekti, kui andmetöötleja poole pealt.
5) Kaitse kogu eluks. Kuna lõimitud andmekaitse on süsteemi sisse toodud juba kohe alguses, siis see tähendab kaitset terveks andmete elueaks.
6) Läbipaistvus ning nähtus. Süsteemi osade tegevus on nähtav nii kasutajale, kui ka levitajale.
7) Kõik toimingud peavad olema kasutajakesksed. Üksikisikute huvidest lähtumine peab olema kõige tähtsam.

[43]Andmekaitse Inspektsioon. Vaikimisi ja lõimitud andmekaitse, 2017. http://www.aki.ee/et/andmekaitse-reform/vaikimisi-ja-loimitud-andmekaitse (12.04.2017)
[44]Rest van, J., Boonstra, D., Everts, M., Rijn van, M., Paassen van, R. Designing Privacy by Design. - Lecture Notes on Computer Science, Privacy Technologies and Policy, 2012, lk 52-77.
[45]Cavoukian, A. Privacy by Design. The 7 Foundational Principles, 2009. https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf (03.03.2017)

Privacy by Design ja *Privacy by* Default rakendamine peaks idee poolt kaasa tooma selle, et edasiselt puudub vajadus andmete kaitseks, mis tähendab seda, et näiteks andmete kolmanda edasitöötluse ajal on subjekti õigused automaatselt tagatud. Andmesubjekti vaatevinklist on kergem, kui asjakohased valikud tehakse eelnevalt ära, sest reeglina puudub tavainimesel teadlikus selle kohta, mis on tema jaoks andmekaitse kontekstis parim.

1.4 Tegevusjuhend privaatsuse kohta m-tervishoiu puhul

Tegevusjuhendi näol on tegemist näitega Euroopa Liidu uuest regulatiivse poliitika suunast, milleks on iseregulatsioon.[46]Tegemist on alternatiivse ning uuendusliku õigusliku instrumendiga, selle asemel, et panna paika kindlad reeglid antakse võimalus erinevate soovituste näol luua iseseisev kontrollmehhanism.[47]
Tegevusjuhendisse saab suhtuda, kui Üldmääruse pikendusse ning lisasse, mis on otseselt seotud andmetöötlus toimingutele m-tervishoiuga seonduvates rakendustes. Ennekõike on tegevusjuhendi fookuses teenuste ning seadmete loojad. Idee sellise lähenemise taga on see ,et lubades tööstusel reguleerida end ise, antakse selleläbi võimalus erinevatele uuendustele, mis muidu jäigemate reeglite paika panemisel võib kaduda.[48]

Tegevusjuhendi peamiseks eesmärgiks on külvata usaldust lõppkasutajate seas ning hõlbustada andmekaitseliste reeglite täitmist.[49] Läbi juhendi on võimalik teha assisteerida rakenduse loojaid nii, et oleks võimalik teha teadlikke valikuid vastavuses Euroopa andmekaitse seadustega. Seaduslooja on otsustanud sellise lähenemise kasuks selletõttu, et et eelduste kohaselt peaksid jooned traditsioonilise tervishoiu ja isekontrollivate seadete vahel

[46]Tikk, E.,.Nõmper,A. Informatsuoon ja õigus. Tallinn: Juura 2007, lk 36-38
[47]Senden, L. Soft-law, self-regulation and co-regulation in European law: Where Do They Meet? - Electronic Journal of Comparative Law, 2005, 9 (1), lk 1-2.
[48]Ruback, T. A Brief Look at Self-Regulation and European Data Protection, 2015. https://iapp.org/news/a/a-brief-look-at-self-regulation-and-european-data-protection/ (12.02.2017).
[49]European Comission. Draft Code of Conduct on privacy for mobile health applications, 2016. http://ec.europa.eu/newsroom/dae/document.cfm?action=display&doc_id=16125 (18.04. 2017).

veelgi hajuma.[50]Ning selleks, et valdkond saaks areneda edasi tuleb toetada üksikisikute õigusi ning võtta vastu meetmeid selle kindlustamiseks. Iseregulatiivse instrumendi valik on parimaks lahenduseks olukorras, kus on vaja aktiivselt panustada majanduse arengusse, sest võrreldes seadustega on loomise protsess oluliselt kiirem ning lihtsam.[51]

Tegemist on heade ning praktiliste juhtnööridega, mis seletavad lahti, kuidas lähtuda Üldmääruses sätestatust. Tegevusjuhend on tavainimese kesknesest juriidilised terminid on lihtsamalt lahti seletatud ning samuti on näidatud kuidas printsiipe kontekstist tulenevalt rakendada. Kontseptsioon on äärmiselt tehnoloogia sõbralik, sest loomisel on kasutatud valdkonnaga seotud olevate ekspertide arvamust. Hetkel on *Code of Conduct* veel ülevaatamisel, kuid eelduste kohaselt peaks see jõustuma koos üldmäärusega. Kuigi tegevusjuhendil näol on tegemist vabatahtliku raamistikuga, on seal sisalduvad ettekirjutused otseselt tulenevad GDPR-ist, mille järgimine on tegelikult ikkagi kohustuslik.

1.5 Kohtulahendid

Nii Euroopa Kohus (ECJ), kui ka EIK on oma vastavates lahendites toonitanud ennekõike seda, et isikuandmete kaitse, sealhulgas meditsiiniliste andmete kaitse on äärmiselt oluline Euroopa Inimõiguste Konventsiooni artikkel 8 seisukohast austada pere- ja eraelu. Terviseandmete konfidentsiaalsuse austamine on vitaalse tähendusega kõikide konventsiooni osapoolte õigussüsteemidele. Seda seeõttu, et terviseteabe avalikustamine võib väga tõsiselt mõjutada inimese era- ja pereelu, samuti sotsiaalsed seisukorda ning töösuhteid. Terviseandmetega seonduva konfidentsiaalsuse austus ei ole tähtis mitte ainult privaatsuse õiguse vaatenurgaks, vaid see suurendab kasutajate usaldust pakutavatesse teenustesse. Ilma sellise kaitseta võib tekkida olukord, kus isik vajab abi, kuid näiteks diskriminatsiooni

[50]European Commission. eHealth Action Plan 2012-2020: Innovative healthcare for the 21st century, 2012. https://ec.europa.eu/digital-single-market/en/news/ehealth-action-plan-2012-2020-innovative-healthcare-21st-century. (12.02.2017)
[51]Mantovani, E., Antokol, J., Hoekstra, M., Nouwt, S., Schutte, N,., Zilgalvis,P., Castro Gómez-Valadés, J-P., Prettner, C. Data Protection and Privacy: (In)visibilities and Infrastructures. Law.-Governance and Technology Series, 2011, 1, lk 88.

kartuses hoidub sellest, kahjustades sellega oluliselt oma tervist. Autori arvates on oluline vaadata ning analüüsida kohtupraktikat, sest see illustreeriv terviseandmete kaitse tähtsust veelgi.

1) Rootsi kodanik proua Lindquist avaldas interneti teel oma kolleegide kohta erinevaid andmeid. Nii telefoninumbreid, aadresse, kui ka nimesid. Kaasa arvatud seda, et üks töökaaslastest oli vigastanud oma jalga ning selle tõttu viibis haiguslehel. EIK analüüsis erinevaid elemente ning leidis, et tegemist on isikustatud teabega ning töötlusega. ECJ leidis , et fakt on jagatud informatsiooni vigastuse kohta läheb terviseandmete avaldamise alla isikuandmete kontekstis vastavalt EIÕk artikkel 8 lõige 1-st. ECJ avaldas arvamust, et mõistet terviseandmed tuleb vaadelda ning tõlgendada nii laialt, et see hõlmaks kõiki aspekte seoses üksikisiku füüsilise ning vaimse tervise suhtes.[52]
2) Teises olulises otsuses sooviti kaebaja poolt tühistada eelnev Euroopa Parlamendi otsus, kus otsustati, et isik pole tööks sobilik arvestades tema meditsiinilist seisundit. Kaebajale pakuti Euroopa Parlamendis tööd, mille tõttu nõudis asutus enda kätte Euroopa Komisjonilt isiku meditsiinilisi andmeid, selle tulemusel tehti vastav järeldus, et kaebaja pole piisavalt terve selleks, et teha tööd parlamendis. Kaebaja väitis, et Komisjonil puudus õigus jagada olemasolevaid meditsiinilisi andmeid ning Parlament oleks ise pidanud läbi viima tervisliku seisundi ülevaatuse. ECJ leidis, et antud olukorras ei antud kaebaja oma nõusolekut selleks, et tema kohta käivaid andmeid edastataks, samuti ei leitud, et ülekanne oleks olnud absoluutselt vajalik. Parlamendil oleks olnud võimalus viia läbi ülevaatus kasutades palju leebemaid meetoideid. Kohus leidis, et tegemist in jällegi EIÕK artikli 8 kohaldamise alaga. Kuna tegemist on põhiõigusega, siis on oluline see, et isiku meditsiiniline seisund oleks salastatud. Andmete edasine saatmine kolmandatele osapooltele, seda isegi juhul, kui tegemist on Euroopa Liidu organiga on vastuolus sätestatud õigusega, olenemata sellest, milleks eelnimetatud andmeid kasutatakse. Selline sekkumine võib olla õigustatud ainult sellisel juhul, kui oleks kooskõlas seadusega ning absoluutselt vajalik demokraatlikus ühiskonnas arvestades huve, mis on seotud riigi julgeoleku, avaliku turvalisuse,

[52]Eko 6.11.2003, C-101/01, Lindquist.

majandusliku heaoluga riigis. Või et ennetada kuritegu ning kaitsta erinevaid õigus ja vabadusi.[53]

3) Kolmas on EIK-i lahend. Leedu suurim ajaleht avaldas oma esilehel artikli seoses AIDS-i levikuga riigi maapiirkondades. Sealhulgas oli artiklis kirjas kohaliku tugikeskuse kinnitus, et kaebajad olid haigusesse nakatanud, samuti olid töötajad teinud spekulatsiooni kaebajate seksuaalelu kohta. EIK leidis, et tegemist on EIÕK artikli 8 rikkumisega, mis omakorda näitas seda, et riigil puudusid endal piisavalt tugevad õigusnormid, et tagada piisav andmete konfidentsiaalsus juba alguses. Kohus põhjendas otsust sellega, et kokkuvõttes nõrgendab selline käitumine inimeste usku ning usaldust pakutavasse teenusesse, mille tõttu ei pruugi inimesed enam teenust kasutada, õõnestates usku privaatsusesse ning tuues kaasa võimaliku diskriminatsiooni.[54]
4) Eraldiseisvalt saab siinkohal vaadata lahendit Hispaania vs *Google Inc*[55], tänu millele loodi uue põhiõigusena õigus unustusele Internetis ning sealt tulenevalt õigus andmete kustutamiseks. Lahendit saab võtta, kui täiendavat tööriista andmekaitseliste õiguste lahti seletamisel. Kaebajale ei meeldinud, et tema nime sisestamisel Google Search otsingumootorisse kuvati kaks linki artiklitele, kus oli avaldatud nii kaebaja nimi, kui ka teade sotsiaalkindlustusvõlgade tõttu arestitud kinnisvara enampakkumise kohta. Sellest tulenevalt nõudis kaebaja, et kas ajaleht või otsingumootor oleks kohustatud lehekülgi eemaldama selleks, et isikuandmed oleksid kaitstud. Otsus oli tähelepanuväärne selletõttu, et läbi selle loodi sisuliselt uus õigus. Lahendil on otsene seos suurandmestiku kasutusega ning andmekaevega (mida autor puudutab järgmistes peatükkides). Lahendis on märgitud, et andmesubjekti õigused kaaluvad üles teenuse pakkuja huvid, millest saab lähtuda ka seoses m-tervishoiuga. Tänu sellele on tavakodanikule antud juurde veel üks instrument, mis ideaali kohaselt peaks suurendama andmesubjekti kontrolli enda kuvandi üle küberruumis.[56]

[53]Eko 5.7.2011, F-46/09, V & Edps v. European Parlament.
[54]Eko. 25.02.2009 , 36919/02), Biruk v. Lithuania; Eko 25.02.2009, 23373/03 Armonas v. Lithuania.
[55]Eko. 13.05.2014, C-131/12, Hispaania v. Google Inc
[56]Inimõiguste Keskus. Eesti Inimõiguste Keskuse aastaaruanne 2014-2015, 2015. https://humanrights.ee/app/uploads/2017/01/EIKaruanne2014.est-veebi.pdf (1.05.2017)

2. Terviseandmete töötlus m-tervishoius

2.1 Terviseandmete määratlus seonduvalt m-tervise valdkonnast

Millenniumi alguses hakkasid nii meedia, elektroonilise sideme, kui ka infotehnoloogia sektorid omavahel kokku koonduma ning assimilatsiooni tekkides sündis uus ärikeskond (sh tervishoiu sektor), mis tõi kaasa endaga küsimusi, mis vajasid lahendamist ning vastavaid regulatsioone. Kui veel 10 aastat tagasi mahtus m-tervishoiu malli vaid nutitelefoni rakendused, on need asendumas järk järgult teistsuguste vahendutega, mis on indiviidiga tihedamalt suhestunud ning mille olemasolust võib teadlik olla ainult kasutaja ise.

Kuigi ametlik definitsioon nii maailma, kui ka Eesti teaduskirjanduses puudub on enamjaolt mõistetud selle all tervishoiule lähenemist läbi erinevate elektrooniliste- ja kommunikatsiooni seadmete.[57]Ehk siis tegemist on erinevate meditsiiniliste ning heaoluga seonduvate programmidega, mille ülesandeks on koguda ning analüüsida kasutaja kohta käivat informatsiooni. Tegemist on tuntuma e-tervishoiu sektori alaharuga, mis on toonud endaga kaasa selle, et informatsiooni ning tervishoiu teenuseid edastatakse puhtalt ärilisel eesmärkidel.[58]

Eelduste kohaselt peaks aastal 2017 kõigist nutiseadmete kasutajatest umbes pool külastama m-tervisega seonduvaid äppe. Rakendusi peaks prognoosi kohaselt olema üle miljoni.[59]Tegemist on globaalse fenomeniga, mida illustreerib IHS-i poolt läbi viidud uuring, mille kohaselt oli aastal 2013, kõige populaarsematel tasuta rakendustel alla laadimisi 231 miljonit.[60]Paberkandjale märgitud terviseandmed on alati olnud suure kaitse all, kuid nüüd

[57]Istepanian, R.S.H., Lacal, J. Emerging mobile communication technologies for health: some imperative notes on m-health. - Proceedings of the 25th Annual International Conference of the IEEE Engineering in Medicine and Biology Society, 2003, 2, lk 1414–1416.
[58]Silber, D. The Case for eHealth, 2003. http://www.denisesilber.com/files/case_for_ehealth03.pdf (23.11.2016)
[59]Research2Guidance. Mobile health app market report 2013–2017: The commercialization of mHealth. Research2Guidance, 2013. http://www.researchandmarkets.com/reports/2497392/mobile_health_app_market_report_20132017_the (03.11.2016)
[60]IHS Markit. The World Market for Sports & Fitness Monitors—2013 Edition, 2013. http://news.ihsmarkit.com/press-release/design-supply-chain/sports-and-fitness-app-market-expand-more-60-percent-five-years (03.11.2016)

mängib rolli see, et traditsionaalset arsti ning patsiendi suhet ei eksisteeri, andmemaht on muutunud oluliselt suuremaks ning ligipääsu võimalus on miljonitel.[61]

Kuna valdkond on ülesehitatud puhtalt terviseandmete kasutusele on sellelt tulenevalt oluline teha selgeks, mida täpsemalt läheb terviseandmete kategooria alla lähtudes m-tervise kontekstist. Mõiste seotus rakendustega on muutnud definitsiooni piiritluse senisest hägusemaks ning keeruliseks. Töögrupp on avaldanud arvamust, et seoses äppidega eksisteerib kahte liike terviseandmeid. Meditsiiniline teave klassikalises võtmes ning kaudselt seotud heaolu andmed.[62]

Näiteks, kui analüüsida nutikellas olevat sammulugemise rakendust, mille ülesandeks on lugeda kasutaja poolt astutud sammud ning distantsi pikkus päeva jooksul, siis sellest tulenevalt võib järeldada, et teabel pole tegelikult mingisugust väärtust. On ääretult vähetõenäoline, et informatsioon astutud sammude kohta avaldaks mõju privaatsuse õigusele ehk sellest tulenevalt puudub vajadus rangema kaitse järele. *Ergo* tegemist on heaolu teabega. See on informatsioon, mis on kaudselt tervisega seotud, kuid millel otseselt pole mingit kaalu. Terviseandmete mõiste alla seoses rakendusega läheb puhtalt meditsiinilises kontekstis olev informatsioon ning samuti andmed, mida kombineerides on võimalik teha omakorda järeldusi kasutaja tervisliku seisundi kohta.

Autorile teadaolevalt puudub hetkel kindel piir, mille järgi oleks võimalik teavet eristada (tegevusjuhendis on olemas küll vastav test, kuid tegemist pole õiguslikult siduva dokumendiga). Hetkel on olemas reaalne oht, et andmeid kategoriseeritakse kergekäeliselt ning valesti, mille tulemil õõnestatakse eksisteerivaid andmekaitselisi standardeid. Samuti peab arvestama võimalusega, et esmapilgul süütuna tunduvad rakendused võivad aja möödudes muutuda ohu allikaks (näiteks, kui andmetöötluse protsess toimub pikemat aega on võimalik selle baasil hinnata inimese tervislikku seisundit).

Töögrupp on vastavalt sellele vastavalt toonud välja kriteeriumid, millest võib juhilduda. On kolm kindlat andmegrupeeringut, mis lähevad terviseandmete kategooria alla. Puhtalt

[61]Cortez, N. The Mobile Health Revolution?- UC Davis Law Review,2014, 4 , lk 1189.
[62]Artikli 29 alusel asutatud andmekaitse töörühm, Working Document 01/2012 on epSOS. 2012. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp189_en.pdf (11.01.2017)

meditsiinilise sisuga andmed; tavapärased heaoluandmeid, kuid mida kombineerides omavahel on võimalik teha tervise kohta järeldusi; ning juba olemasolevad järeldused.[63]

Euroopa Andmekaitse Inspektor on andnud omakorda olukorrale hinnangu, et ei tohiks siinkohal andmete tundliku loomuse tõttu siiski üldistada, millised andmed on traditsioonilised terviseandmed ja heaoluandmed. Ideaalis saab täpsema hinnangu anda ainult sellisel juhul, kui analüüsida konkreetseid rakendusi ning asjaolusi.[64] Kui selline hinnang puudub, tuleb siiski suhtuma ja kohaldama terviseandmete mõistet sama laialt, kui seda on kirja pandud. Rolli mängib samuti, miks ja kuidas on andmekogumine toiminud.[65]

Teiseks oluliseks tahuks m-tervise puhul on see, et rakendustest saadav informatsioon oleks võimalikult täpne, sest vastavalt sellele võivad nii arstid, kui ka kasutajaid eraldi järeldusi teha. Kahjuks on olemas ainult limiteeritud kirjandust rakenduste täpsuse kohta, olemasolevate artiklite sisu on väga spetsiifiline ja selle järgi järeldusi teha ei saa. Hetkel läbiviidud uuringud on siiski näidanud, et kerkinud on esile mitmesuguseid meditsiinilisi rakendusi, mis võivad ohustada inimese tervislikku seisundit halva täpsuse tõttu.[66]Kuid see puudutab juba puhtalt meditsiini valdkonda, millest tulenevalt autor teemat ei puuduta pikemalt.

Autor on arvamusel, et erinevad organid peaksid leidma kokkuleppe, mitte andma erinevaid ja üksteist vastandavaid arvamusi. Arvesse peab siinkohal võtma samuti seda, et kuigi Euroopa Liidus eksisteerivad kõrged andmekaitsestandardid, siis liidu välistel riikidel pruugivad need puududa (kasutades pilvetehnoloogiat on näiteks raske hinnata, millise riigi õigust kohaldada, kuna otsesed piirid puuduvad).[67]Liidul on plaan arendada nii e-tervishoiuga seonduvaid

[63]Artikli 29 alusel asutatud andmekaitse töörühm. Annex - health data in apps and devices, 2011. http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150205_letter_art29wp_ec_health_data_after_plenary_annex_en.pdf (11.01.2017)

[64]European Data Protection Supervisor. Opinion 1/2015 Mobile Health. Reconciling technological innovation with data protection, 2015. https://edps.europa.eu/sites/edp/files/publication/15-05-21_mhealth_en_0.pdf (11.01.2017).

[65]Artikli 29 alusel asutatud andmekaitse töörühm, Working Document 01/2012 on epSOS. 2012. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp189_en.pdf (11.01.2017)

[66]Velsen van, L., Beaujean, DJ,. Gemert-Pijen van, JE. Why mobile health app overload drives us crazy, and how to restore the sanity.- BMC Medical Informatics and Decision Making, 2013, 1, lk 13.

[67]Frazee,J; Finley,M; Rohack, JJ. mHealth and Unregulated Data: Is This Farewell to Patient Privacy.- Indiana Health Law Review, 2016, 13 (2), lk 384.

teenuseid, kui ka mõisteid ehk siis autor ei oska hetkel prognoosi anda, kas tulevikus antakse täiendavad juhtnöörid ning definitsioon vastavalt vajadusele.

2.2 Suurandmestiku ning andmekaeve kasutus seoses terviseandmetega

M-tervishoiu puhul on tegemist unikaalse nähtusega, sest see ei piirdu vaid esmase andmetöötlusega. Teatud juhtudel on võimalik andmetöötlus ka peale esimese töötluse lõppu, see läheb *Big Data* ehk suurandmete kasutamise alla. Suurandmestiku puhul on tegemist ülisuure andmemassiga, mis võib koosneda miljonist erinevast allikast ning mida ei saa analüüsida kasutades tavapärast tehnoloogiat. Selleks, et nähtust kirjeldada paremini, lähtutakse reeglina kolmest eraldiseisvast osast – maht, andmevormingute paljusus, andmete tekkimise ning töötlemise kiirus.[68]

Tekkinud ärimudelid kasutavad uusi võimalusi seoses isikuandmete massilise kogumise ning kiire edastamisega. Samuti on võimalik andm eid kombineerida ning korduvalt kasutada ettenägematutel eesmärkidel, mille tõttu on seatud andmekaitselised põhimõtted täiesti uutele alustele, mis nõuab omakorda põhjalikku kaalumist, kuidas isikuandmete kaitse põhimõtteid vastavalt rakendada. Tehnoloogial ei tohiks olla võimu, et teha vastavaid ettekirjutusi, millised peaksid olema ühiskonna väärtused ning õigused. Kuid samal ei tohiks pidada põhiõiguste säilitamist ning innovatsiooni soodustamist omavahel vastuoluliseks.[69]Kuigi tegemist on hetkel veel väheesineva tehnoloogilise trendiga ei tohiks seda seetõttu alahinnata.[70]

Suurandmestiku puhul on nõrgaks kohaks, et aja jooksul kogutakse aina rohkem andmeid, mille tulemusena on võime teha vahet kasutul ja kasulikul teabel raskendatud. Seda selletõttu,

[68]Euroopa Andmekaitseinspektor. „Suurandmetega kaasnevad probleemid: üleskutse läbipaistvusele, kasutajate kontrollile ja andmekaitsele disaini ning aruandekohustuse abil", 2016. https://edps.europa.eu/sites/edp/files/publication/16-02-20_challenges_of_big_data_et.pdf (14.01.207)

[69]Ibid.,lk 5

[70]Bosco, F., Creemers, N., Ferraris, V., Gaugin, D., Koops, BJ. Profiling Technologies and Fundamental Rights and Values: Regulatory Challenges and Perspectives from European Data Protection Authorities. Reforming European Data Protection Law. Dordrecht: Springer, 2015, lk 4.

et kogutavad andmekogumid ületavad inimmõistuse piirid.[71]Subjekt võib anda esmaseks töötluseks nõusoleku, kuid tihtipeale tähendab suurandmete protsesseerimine seda, et isikuandmeid kasutatakse kas teisel otstarbel või edastatakse kolmandatele osapooltele.[72]

Suurandmestiku kasutus võib iseenesest olla täiesti ohutu, sisaldades mitte mingisuguseid isikuandmeid.[73]Samas suurandmete analüüs seonduvalt rakendustega on näidanud, et tegemist on siiski isikuandmete töötlusega, mille tõttu on kõikidel osapooltel tulenevalt GDPR-ist kogustus järgida isikuandmete töötkusega seonduvaid põhimõtteid.

Suurandmete kogumisel moodustatakse hiiglaslik teabetaristu, mida on raske hoomata. Et selliseid andmehulki töödelda, on vaja kasutada väga spetsiifilist tehnoloogiat, mille nimeks on *data mining* . Andmekaeve on tegelikult profileerimine, mille eesmärgiks on analüüsida andmehulka ning selle tulemil moodustada võimalikult sarnase näitajatega rühmitusi. Kui andmeid struktureerida vastavalt, siis on läbi valemite leida nii kasutaja käitumismuster, kui ka tulemuse tõenäolisus.[74]Käitumismustri arvutamisel suudetakse ette näha, mida isik võib tulevikus tahta, enne kui inimene ise sellest teadlik on. Tegemist on valdkonnaga, mille keskseks ideeks on leida üles teavet, mida traditsiooniliste meetmete rakendamisega kätte ei saa.

Andmekaitse seisukohast on kõige olulisemaks faktoriks see, et läbi andmekaeve meetiodi teostuse on informatsiooni võimalik läbi töötada nii, et igasugune teave on lõpuks ikkagi isikustatud (uuringud on näidanud, et sellised kaitsemeetmed nagu näiteks anonümiseerimine ning esmane krüpteering ei ole enam efektiivsed), mis omakorda toob kaasa usu nõrgenemise privaatsusesse.[75]

Mida rohkem suurandmestikke aja jooksul tekib, seda suurem on tõenäosus, et inimest on võimalik identifitseerida, sest suurandmestiku hulgad on omavahel tihedalt soetud. Samuti

[71]Cukier, K., Mayer-Schoenberger, V. The Rise of Big Data. How It's Changing the Way We Think About the World. Foreign Affairs 2013 : nr 92 (3), lk 28-29.
[72]International Commissioner's Office. Big data, artificial intelligence, machine learning and data protection, 2016. https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf (03.01.2017)
[73]Andmekaitse Inspektsioon. Suurandmed ja privaatsus ,Juhendmaterjal organisatsioonidele, 2017. http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/suurandmed_ja_privaatsus.pdf (16.02.2017)
[74]Liiv, E. Kas eraisikul on õigus unustusele Internetis? Juridica 2014, 9, lk 643-651.
[75] Tene,O., Polonetsky, J. Privacy in the age of big data: a time for big decisions. Stanford Law Review Online, 2012, 64, lk 16.

peab arvestama sellega, et kui terviseandmed satuvad valedesse kätesse, siis on nende läbi võimalik sooritada erinevaid tehinguid. Näiteks võib tekkida olukord, kus andmeid müüakse edasi kindlustuskompaniidele, kes võivad isikutele keelata katvuse või farmaatsia organisatsioonidele, kes vastavalt isiku tervislikule seisundile määravad vastava hinna.[76]Sellest võib omakorda järeldada, et olemas on otsene lüli terviseandmete ning kasumi vahel, mis on problemaatiline.

Kui täiendavalt analüüsida suurandmestiku otstarvet, siis tundub, et tegemist on nähtusega, mis on otseses vastuolus andmekaitseliste põhiprintsiipidega. Seda selletõttu, et andmeid kohutakse olulisemalt suuremal määral, säilitusaeg on senisest pikem ning on võimalus kasutada mitmed erinevat moodi sõltumata esmasest eesmärgist Seetõttu on autori arvates põhjendatud küsimus, kas traditsioonilised andmekaitse printsiibid on kohaldatavad. Töögrupp on olukorrale üritanud anda selgust, andes mõista, et ei ole põhjust arvata seda, et liidu sisesed andmekaitse põhimõtted ei ole antud juhul kehtivad ning suurandmestiku kasutuse arendamiseks sobilikud. Selle asemel tuleks otsida mooduseid, kuidas sisse tuua vastavaid parandusi, ning praktikas muuta printsiipide rakendust senisest efektiivsemaks.[77]

Euroopa Andmekaitse Inspektor on omakorda avaldanud arvamust, et selleks, et säilitada fundamentaalsete õiguste kaitse, tuleks väljakujunenud põhimõtteid arendada edasi uuel moel, sest eesmärgid on jäänud ikkagi samaks.[78] Lisades, et andmekaitse põhiprintsiibid nagu läbipaistvus, proportsionaalsus ja eesmärgi pärasus annavad hea aluse selleks, et suurandmestiku ajastul kaitsta üksikisiku õigusi. Sellest olenemata on olemas vajadus uute komplimenteerivate printsiipide järgi, mis täiendaksid olemasolevaid printsiipe, mis on hetkel väljendunud GDPR-is vastutuse suurendamisega ning privaatsuse vaikimisi ning lõimimisi põhimõttega.[79]

---

[76]Corbin, K. What happens with data from mobile health apps?, 2015 http://www.cio.com/article/2903573/healthcare/what-happens-with-data-from-mobile-health-apps.html (13.11.2016)

[77]Artikli 29 alusel loodud andmekaitse töögrupp. Statement on Statement of the WP29 on the impact of the development of big data on the protection of individuals with regard to the processing of their personal data in the EU, 2014. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp221_en.pdf (13.04.2017)

[78]Tene,O., Polonetsky, J. Privacy in the age of big data: a time for big decisions. Stanford Law Review Online, 2012, 64, lk 16.

[79]Euroopa Andmekaitse Inspektor. Meeting the challenges of big data. A call for transparency, user control, data protection by design and accountability, 2015. https://edps.europa.eu/sites/edp/files/publication/15-11-19_big_data_en.pdf (13.04.2017)

Autor nõustub seisukohaga, suurandmestiku ulatuslik kasutamine võib endaga kaasa seniste põhiväärtuste õõnestamise. Sellest tulenevalt on vajalik võtta kasutusele täiendavad meetmed, mis on tuletatud olemasolevatest õigustest.

2.3 Pilvetehnoloogia

M-tervishoiu teenuseid on võimalik pakkuda ka läbi pilveteenuste kasutamisega. Pilvetehnoloogia näol on tegu teenusega, mis kasutab andmetöötlus toimingute läbiviimiseks ning salvestamiseks suuri andmekeskuseid ehk servereid, millele on võimalik ligi pääseda ainult spetsiaalset tarkvara kasutades.[80]Tegemist on teenusemudeliga, millega kaasnevad sarnased probleemid nagu suurandmestikuga.[81]

Esiteks võib pilvel olla mitu kasutajat samaaegselt ehk siis kasutaja andmetele omab ligipääsu korraga mitu inimest. Teiseks on teenuse pakkujal on omakorda võimalus mängida pilves oleva teabega ning jälgida, mida kasutajad keskkonnas teevad.[82] Sellest tulenevalt on hajunud traditsioonilise andmetöötleja mõiste. Andmekaitse Inspektsioon on öelnud, et isikuandmete töötlemise seisukohalt on teenuse kasutaja vastutava töötleja rollis, volitatud töötajaks on pilveteenuse osutaja. Sellelt tulenevalt on tavakasutajal rohkem kohustusi. Autori hinnangul muudab pilvetöötluse kasutamise problemaatiliseks faktor, et kindlad riigipiirid puuduvad, mille järgi oleks võimalik hinnata, millise riigi õiguse kohaldamisalaga on tegu. Euroopa Liidul võivad eksisteerida tugevad andmekaitselised standardid, kui kolmandates riikides nii ei pruugi olla.

Andmekaitse Inspektsiooni IT nõunik on avaldanud arvamust, et enne pilvandmetöötluse kasuks otsustamist tuleb kasutajal esmalt teostada igakülgne ja põhjalik riskianalüüs, mis

[80]Andmekaitse Inspektsioon. Pilvandmetöötlus, 2014. http://www.aki.ee/et/pilvandmetootlus (13.04.2017)

[81]European Digital Rights. An introduction to data protection, 2013. https://edri.org/files/paper06_datap.pdf (12.04.2017)

[82]De Filippi, P., Belli, L. Law of the Cloud v Law of the Land: Challenges and Opportunities for Innovation. – European Journal of Law and Technology 2012, 3 (2), lk 2.

autori arvates ei ole kõige paremaks lahenduseks. [83]Tavainimesel reeglina puuduvad vastavad teadmised, et riskianalüüsi teostada.

Kuna digikeskonnast tulenevalt on andmetöötluse võimalused oluliselt suuremad siis sellest järelduvalt peavad üksikisikute õigused olema paremini tagatud, hetkel veel vastavad tugevad raamitingimused selleks puuduvad. Kuigi Euroopa Liit on võtnud suuna digitaalmajanduse arendamisele, mille läbi nõutakse liikmesriigilt tugeva digitaalteenuste koordinaatorite võrgustiku rajamist, mis võib olukorda oluliselt parandada.[84] Andmekaitse Inspektor Giovanni Buttarelli on öelnud, et ettevõtted peaksid siinkohal proovima ise teha jõupingutusi selleks, et leida uuenduslikke viise, mille läbi rakendada andmekaitse põhimõtteid, millega autor nõustub.[85] Hetkel on isikul küll võimalus olemas osaliselt kontrollida isikuandmete töötlust läbi pilveteenuse, kuid tulevikus peaks selguse nimel tõmbama otsesemaid piire.

[83]Andmekaitse Inspektsioon. Pilvandmetöötlus, 2014. http://www.aki.ee/et/pilvandmetootlus (13.04.2017)
[84]Euroopa Ülemkogu. Järeldused, 2014. http://www.riigikogu.ee/?op=emsplain&page=pub_file&file_id=5e49dedb-09a1-479b-acbf-09ef47bf0897&.pdf (18.04.2017)
[85]Euroopa Andmekaitse Inspektor. Euroopa Andmekaitseinspektori arvamuse kokkuvõte teemal „Suurandmetega kaasnevad probleemid: üleskutse läbipaistvusele, kasutajate kontrollile ja andmekaitsele disaini ning aruandekohustuse abil", 2016. https://edps.europa.eu/sites/edp/files/publication/16-02-20_challenges_of_big_data_et.pdf(18.04.2017)

3. Olemasoleva õigusliku raamistiku täiendav analüüs seoses m-tervishoiuga

Kiire tehnoloogiline areng ja üleilmastumine on tekitanud isikuandmete kaitsel uusi väljakutseid, sest isikuandmete kogumise ja jagamise ulatus on märkimisväärselt suurenenud. Tehnoloogia võimaldab nii era- kui ka avaliku sektori asutustel kasutada isikuandmeid oma tegevuses enneolematus ulatuses.

Nende muudatuste tõttu oli liidus vaja tugevat ja ühtsemat andmekaitseraamistikku ning selle täitmise tõhusat tagamist. Meditsiinisektori arenguga on kasvanud m-tervishoiu kandev roll, mis otseselt ei pruugi olla halb. Tehnoloogia ja tervishoidu omavaheline põimumine aitab vähendada tehtavaid kulutusi, annab patsiendile suurema ja parema ülevaate oma tervishoiu teenuste üle ning lihtsustab juurepääsu nii arstiabile, kui ka erinevale teabele, ka ei mängi geograafiline asukoht mitte mingisugust rolli patsiendi ja arsti rolli suhtes. Kuna tervishoiu süsteemid peavad vastu astuma sellistele katsumustele nagu krooniliste haiguste osakaalu suurenemine ja vananen populatsioon, samaaegselt arvestades eelarveliste kärbetega võib m-tervishoiu arendamine pakkuda vastavat lahendust.[86]

Samasuguse seisukoha on võtnud Europa Andmekaitse Inspektor. M-tervishoid pakub rikkalikult võimalusi tervishoiu sektori reformatsiooniks, aidates ennetada haigusi, andes ettevõtetele suuremaid võimalusi ning madaldada tervishoiule tehtavaid kulutusi. Selleks, et valdkond areneks täiskiirusel edasi on aga vaja leppida võimalustest tulenevate kohustustega seoses privaatsuse tagamisega.[87]

Nutitelefonide ökosüsteemide areng on toonud endaga kaasa suurel hulgalt kontekstist mitte teadlikke rakendusi, mida saab vaadelda kui kasutaja andmete ülemäärase kogumisena. Väide, et iga rakenduse pakkuja vajab ligipääsu andmesubjekti andmetele (kõnelogi, asukoht, fotod), et teenust üleüldse kasutada on ülemäärane ja kontrollimatu. Uuringud on näidanud, et

[86]GSMA. mHealth and the EU regulatory framework for medical devices, 2012 ://www.gsma.com/connectedliving/wp-content/uploads/2012/03/mHealth_Regulatory_medicaldevices_10_12.pdf (16.04.2017)

[87]Euroopa Andmekaitse Inspektor. Euroopa andmekaitseinspektori arvamuse kokkuvõte teemal „Mobiilne tervishoid: tehnoloogilise innovatsiooni ühitamine andmekaitsega", 2015. https://edps.europa.eu/sites/edp/files/publication/15-05-21_mhealth_summary_et.pdf(16.04.2017)

tihtipeale puudub kasutajal teadlikus äppide kogutavate andmete kohta, kuid sellest teada saades on reeglina järgnenud negatiivne reaktsioon.[88]

Kuna isikuandmete kaitse õigus on põhiõigus, siis seadus peab kaitsma isikut kui nõrgemat poolt, millele vastavalt on sõnastatud ka andmekaitseseaduste eesmärgid.[89]Esmaselt saab juhilduda m-tervise reguleerimisel rahvusvahelistest instrumentidest. Õigus privaatsusele on andmekaitse lähtekohaks ning mis tuleb vastavalt EIÕK artikli 8-st. Täiendavalt on õigus eraelule toodid välja samas sõnastuses Hartas, mille artikkel 8 toob omakorda välja andmekaitse, kui eraldiseisva põhiõiguse.[90]

Kuigi nii EIÕK-is, kui harta artikkel 7-s pole sätestatud õigust andmekaitsele *expressis verbis* on seda siiski võimalik tuletada.[91] EIÕK-i näol on tegu kõige olulisema dokumendiga liidu tasandil, kuigi võib väita, et oma vanuse tõttu ei ole tegemist enam relevantsete sätetega on nii Euroopa Komisjon, kui ka EIK seisukohal ,et sätteid on võimalik kohaldada tänase päeva tingimustes arvestades EIÕK-ist tulenevat eesmärki ning abstraktset sõnastust. Konstitutsioonilisest vaatenurgast ei ole oluline mitte andmete kaitse *per se,* vaid inimväärikusest tulenevate õiguse ning vabaduste kaitse.[92]Kuigi andmekaitse ning privaatsust ei saa võtta, kui üksteise sünonüümi, sest andmekaitseõigusega seonduvad mitmed eripärad.[93]Siiski tulenevalt sellele on andmekaitse õigusel tugev alustala ning seadusandjal on kohustus tagada isikute õiguste ning vabaduste kaitse.

Andmekaitselised reeglistikud paneb üldiselt paika Isikuandmete Kaitse Üldmäärus (kuigi hetkel kehtib veel vana direktiiv ei uuri autor töös seal tulenevaid sätteid). Kui juhinduda meditsiinis eksisteerivast eetikast, siis tuleb lähtuda autonoomsuse printsiibist, mille

[88] Boyles, J.L,. Smith, A., Madden, M. Privacy and Data Management on Mobile Devices, 2012. http://www.pewinternet.org/2012/09/05/privacy-and-data-management-on-mobile-devices/ (10.11.2016)
[89]Stark, P. Privacy, Big Data, and the Public Good: Frameworks for Engagement. Cambridge: Cambridge University Press 2014, lk 5-43.
[90]Kokott, J., Sobotta, C. The distinction between privacy and data protection in the jurisprudence of the CJEU and the EctHR. International Data Privacy Law, 2013, 3 (4), lk 222.
[91]Bygrave, L.A. Data Protection Pursuant to the Right to Privacy in Human Right Treaties.- International Journal of Law and Information Technology 1998, nr 6 (3), lk 255-259.
[92]Kranich, H. Ühiskonna (eba)normaalne areng ja inimõigused. Nimede kohtulahendites avalikustamise näide. Juridica, 4, 2015, lk 277-289.
[93]Lynskey, O. Deconstruction Data Protection: The „Added-Value" of a Right to Data Protection in the EU Legal Order.- International & Comparative Law Quarterly, 2014, 63 (3), lk 597.

olemasolu toetab patsiendi individuaalseid väärtusi.[94] M-tervishoiu kontekstis kandub see üle sellisesse võtmesse, et kasutajaid ei tohi millekski sundida ega petta, vaid isik peab olema teadlik ning informeeritud teda puudutava kohta.[95]

Kuigi tegemist on uudse valdkonnaga tuleb siiski andmetöötlusel lähtuda ettenähtud printsiipides - läbipaistvus, legitiimsus ning proportsionaalsus. Äppide puhul on kõige olulisemaks elemendiks, mille kaudu on seaduses sätestatud tingimused täidetud subjekti nõusoleku saamine. Kuigi Euroopa Andmekaitse Inspektori kohaselt on hetkel veel ebaselge, mida täpsemalt tähendab seaduses ettenähtud ühene ning selge nõusolek.[96]Selleks, et nõusolekut töötluseks saada on reeglina vajalik privaatsuspoliitika olemasolu. Kuid vaadata üldmäärust, siis on seal antud soovituseks, et privaatsuspoliitika võiks endas hõlmata kas vajaliku lahtri märgistamist või muud avaldust, milles väljendub sõnaselge nõusolek. Tulenevalt läbipaistvusprintsiibist tuleb eelnevalt kasutaja tehe selgeks samut miks ja kuidas andmetöötlus toimib.

Legistatsiooni poole pealt ei ole kõige targemaks küsimuseks ehk see, miks inimesed kasutavad edasi selliseid platvorme või teenuseid vaatamata oma privaatsuse kompromiteerimisest. Vaid pigem see, kuidas soodustada võimalust selleks, et kasutaja saaks näha ja otsustada, mida täpsemalt edastatakse, säilitades selle läbi oma digitaalset kohalolu ning ligipääsu võrgule.

Kuigi tegemist on efektiivse ning positiivse lahendusena peab arvestama sellega, et teatud limiidini on andmesubjektil võimalik kontrollida ning meeles pidada, millele täpsemalt on nõusolek antud. Hetkel on nii, et iga alla laaditud rakendusega sõlmib kasutaja sisuliselt uue lepingu, aja möödudes ning rakenduste hulga suurenedes on kasutajal raske kontrollida ning meeles pidada, millele nõusolek antud on. Olenemata sellest on autor arvamusel, et läbipaistvuse printsiibi sisse toomine suurendab olulisel määral subjekti võimet kontrollida enda kohta käivat teavet.

---

[94] Soosaar, S. Inimese autonoomia ja informeeritud nõusolek kui protsessid, 2004. http://andressoosaar.planet.ee/autonoomia%20&%20consent%20kui%20protsessid.pdf (16.03.2017)

[95]Mantovani, E., Quinn, P. mHealth and data protection – the letter and the spirit of consent legal requirements. -International Review of Law, Computers and Technology ,2014, 28 (2), lk 222-236.

[96]Euroopa Komisjon. Komisjoni teatis Euroopa Parlamendile, Nõukogule, Majandus- ja sotsiaalkomiteele ning regioonide komiteele. Terviklik lähenemisviis isikuandmete kaitsele Euroopa Liidus, 2010. http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_et.pdf (23.01.2017)

GDPR on revolutsiooniline selletõttu, et esmakordselt on toodud sisse tehnoloogiliste trendidega arvestavad mõisted nagu *Privacy by Design* ja *Privacy by Default*. Selleks, et tagada parim kaitse on üritatud läheneda probleemile juba algfaasis.[97] See tähendab seda, et rakenduse looja peab teenust disainides tegema parimad valikud selleks, et oleks tagatud andmete maksimaalne kaitse automaatselt. See on kasutajasõbralik lähenemine ühiskonnas, kus kasutajad käivad enda kohta käiva informatsiooniga väga kergelt ringi. Eelnevalt oli vaid Andmekaitse Inspektsioonil kohustus jälgida kõiki rakendustega seonduvat, mis praktikas ei ole efektiivne, selletõttu on paremaks lahenduseks see, et protsessi teistel osapooltel on olemas seadusest tulenevad lisakohustused. Seda toetab omakorda Andmekaitse Inspektor Giovanni Butarelli on välja toonud arvamus, et EL seadusandja peaks edendama vastutuse jaotamist osapooltele, kes on tihedalt rakenduste loomisprotsessiga seotud.[98]Mida GDPR-i uus printsiib sisuliselt teeb.

Sellised meetmed aitavad kindlustada kõrgete andmekaitse standardite järgimise arvestades suurandmete ning pilvetehnologia kasutusele võttu. Olemasolevaid ideid on samamoodi konkretiseeritud, selleks, et tagada efektiivsem kaitse. Eesmärgi piirangu mõiste, minimaalse andmekogumise põhimõtte, vastutava töötleja kohustused *etc*.

Üldmääruse peamiseks eesmärgiks on anda nutitelefonide, sotsiaalmeedia ja internetipanganduse ajastul kodanikele parem kontroll oma andmete üle, mille tõttu on toodud fokuseeritum ja konkreetsem lähenemine üksikisikute kaitsele. Sellest tulenevalt on laiendatud andmekaitse õiguse reegleid ka kõikidele ettevõtetele, mis baseeruvad väljaspool liidupiire. Tänu seadusest tulenevale positiivsele kohustusele peavad välismaised rakenduste loojad tagama senisest tugevama kaitse, mis on kindlustatud senisest suuremate trahvidega.

Üldmääruse loomise idee võtab kokku Peter Hustinixi, endise andmekaitseinspektori arvamus. IKT annab võimalusi juurde põhimõtteliselt igas eluvaldkonnas, mis on suurema tähtsusega. Selletõttu on ääretult oluline ,et Euroopa Liit teeks endast kõik olenema, et toetada IKT arengut ning kasutust. Digitaalse keskkonna arenemissuuna keskmes on seisukoht, et kõik peab lähtuma ennekõike üksikisikutest ning nende kaitsmisest, sest see toob kaasa

[97]Hustinix, P. Privacy by design: delivering the promises. Identity in the Information Society, 2010, Volume 3, Issue 2: Springer Publishing, lk 253–255.
[98]Euroopa Andmekaitse Inspektor. Euroopa andmekaitseinspektori arvamuse kokkuvõte teemal „Mobiilne tervishoid: tehnoloogilise innovatsiooni ühitamine andmekaitsega",2015. (16.04.2017)

kasutaja usalduse, mis omakorda soodustab ning suurendab uute teenuste kasutusele võtmist.[99]

Sellest tulenevalt on autor jõudnud töös järeldusele, et kuigi andmekaitse regulatsioonidel on olemas mõningased puudused, on nad siiski kohaldatavad m-tervise valdkonna suhtes.

Seaduses on märgitud senisest laiem kohaldamise ala, mille eesmärgiks on olla vastavuses tehnoloogiaga, selletõttu ei tohi olla seaduses defineeritud mõisted ammendava sisuga. Reeglina on õiguse loomise protsess ääretult aeglane, mis tähendab seda, et olemasolevad õiguslikud instrumendid peavad olema hästi kohaldavad ka pikaajaliselt ning ülikiiresti muutuvate tingimuste suhtes. Vajadus konkreetse õiguse järgi m-tervishoiu valdkonnas tegelikult puudub. Samuti saab juhinduda Tegevusjuhendis välja toodud juhtnööridest, mis tagab selle, et terviseandmed oleksid efektiivselt kaitstud.

Autori arvamust toetab omakorda Andmekaitse Inspektsiooni poolt viidud läbi olukorra hindamine, kus uuriti isikuandmete töötluse korda, leitavust ning arusaadavust ning leiti, et üldjoontes on isikuandmete kaitse nutiseadmete rakendustes tagatud.[100]Samuti on olemas võimalus sertifitseerida platvorm järelvalveorganite poolt, mis tagab selle, et andmekaitselised nõuded oleksid tagatud.

Tuleviku tarbeks on autor arvamusel, et tuleks selgeks teha, millisel juhul on tegemist meditsiiniliste seadmetega, mida reguleeritakse vastavate eriseadusega. Seega, kui rakendus või seade, kvalifitseerub meditsiiniseadme alla kaasnevad sellega rakenduste arendajatele ning tootjatele eraldi kohustused selleks, et näidata, et tegemist on kvaliteetse tootega, mis ei ohusta inimesi. Autor on seisukohal, et kui äpp läheks meditsiini seadme kategooria alla, siis sellest tulenevalt oleksid andmekaitse reeglistikud automaatselt paremini tagatud. Sellest tulenevalt võiksid idee kohaselt m-tervishoidu reguleerida lisaks e-kaubanduse direktiiv, meditsiiniseadmete direktiiv ning e-privaatsuse direktiiv.

[99]Euroopa Komisjon. Euroopa Komisjoni teatis Euroopa Parlamendile, Euroopa Majandus- ning Sotsiaalkomiteele ning Regionaal komiteel. Euroopa Digitaalne Majanduskava, 2010. http://eur-lex.europa.eu/legal-content/et/ALL/?uri=CELEX:52010DC0245R(01) (18.04.2017).
[100]Andmekaitse Inspektsioon. 2014. a interneti rehitsemise päeva seire kokkuvõte,2014. http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/Interneti%20seire%20p%C3%A4eva%20kokkuv%C3%B5te%20%28l%C3%B5plikI%29.pdf (20.04.2017)

Kokkuvõte

Autori bakalaureusetöös selgub ennekõike tugev seos IKT ning andmekaitselise raamistiku vahel, IKT arenduse üheks kriteeriumiks on andmekaitsega seotud tingimused.. Moodne andmekaitse sai aluse tänu andmetöötluse muutumisele seoses 1970nendate aastate tehnilise revolutsiooniga. Nutiseadmete kasutamine on muutunud tänapäeva elu üheks lahutamatuks osaks, statistika kohaselt omab üle poole Eesti elanikkonnast nutiseadmeid. Nutitelefonide kasutamine on üles ehitatud rakenduste ehk äppide kasutamise võimalusele. Nad võimaldavad pakkuda mitmesuguseid erinevaid teenuseid, mis kõik toimivad isikuandmete töötlemise ning kogumise alusel. Rakenduste eri kategooria moodustab mobiilne tervishoid, tegemist on üsna uue märksõnaga, mille all mõistetakse erinevate tervishoiu teenuste pakkumist läbi nutiseadmete, millega kaasnevad andmekaitse tingimuste rikkumised.

Bakalaureusetöö keskseks eesmärgiks oli uurida erinevate andmekaitse õiguslike normide sobivust ning kohaldatavust m-tervishoiu valdkonnas. Millest tulenevalt on uurimistöö keskseks küsimuseks ning hüpoteesiks, kas olemasolevad andmekaitse õiguslikud sätted on piisad selleks, et tagada kõike efektiivsem kaitse m-tervishoiu puhul. Kuigi hetkel kehtib veel direktiiv 95/46/EÜ on autor lähtunud töö kirjutamisel ennekõike Isikuandmete Kaitse Üldmäärusest.

Tegemist on keerulise ning laia valdkonnaga, mida illustreeriv fakt, et mobiilse tervishoiu kategooria alla lähevad nii rakendused, kuhu isik võib ise salvestada enda kohta käivat teavet, kui ka seadmed, millel on olemas võimalus läbi lokaalsete sensorite ligi pääseda kasutaja kohta käivatele parameetritele ning selle baasil teha vastavaid järeldusi. Kuna tegemist on tundliku teabega, mida m-tervishoiu sektoris kasutatakse, tuleb lähtuda olulisemalt rangematest nõuetest, kuid andmekaitse standardite järgimine võib valdkonna uudsuse tõttu olla raskendatud.

Käesolev bakalaureusetöö on üles ehitatud Euroopa Liidu andmekaitseõigusele, millele on vastavalt lisatud erinevate andmekaiste organisatsioonide arvamusi selleks, et õigusnormide sisustada ning anda parem ülevaade. Töös on kasutatud suuremas osas välismaiseid internetist leiduvaid allikaid ja seda selletõttu, et autorile teadaolevalt ei ole Eesti teaduskirjanduses

valdkonda uuritud. Antud töös on kasutatud mõningaid kaudselt teemaga seotud Juridica artikleid ning mõningaid varasemate analoogseid tööde materjale. Sellest tulenevalt on töö jagatud kolmeks eraldi seisvaks peatükiks.

Esimeses peatükis annab autor ülevaate olemasolevast õiguslikust raamistikust, samuti kaardistatakse valdkonna kesksed mõisted, milleks on isikuandmed ning terviseandmed. Andmekaitse on tihedalt suhestunud privaatsuse mõistega, mida saab pidada üheks kõige tähtsamaks ning enim tunnustatud õiguseks liidus oma otsese seose tõttu inimväärikusega. Õigus era- ja pereelu puutumatusele tuleneb nii EIÕK artikkel 8-st, kui ka Harta artikkel 7-st. Kui sõnastuses puudub otsene seos andmekaitse õigusega on siiski nii Euroopa Komisjon, kui ka läbi erinevate kohtulahenditele jõutud järeldusele, et mõistetel on otsene seos, mille tulemusel on võimalik ühte tuletada teisest. Eraldi seisva põhiõigusena on isikuandmete kaitse eraldi välja toodud Harta artikkel 8-s. Kuigi võib väita, et tegemist ei ole kõike proaktiivsemate lahendustega on autor arvamusel, et tänu Euroopa Kohtu ning Euroopa Inimõiguste Kohtu lahendite tulemusel tuleb võtta sätteid, kui elavat instrumenti, mida võib vastavalt eesmärgile kohaldada.

Andmekaitse õiguse keskseks mõisteks on isikuandmed, ning bakalaureusetöö teemast tulenevalt terviseandmed. Isikuandmete alla läheb igasugune teave tuvastatud või tuvastatava füüsilise isiku kohta. Tegemist on laia mõistega, kuid seda on seadusandja põhjendanud sellega, et potentsiaalselt võib igasugune teave olla isikustatud, mille tõttu ei tohiks ammendavat nimekirja anda. Isikuandmete eraldi kategooriaks on delikaatsed andmed, mille alla kuulub ka terviseandmete mõiste. Tegemist on andmeliikidega, mis on oma tundlikust natuurist tulenevalt olulisemalt rangema kaitse all. Seda seetõttu, et tegemist on teabega, mida valesti kasutades on oluliselt suurem oht kahjustada inimese põhiõigusi ning vabadusi.

Eelnevalt oli andmesubjekti õigused ning töötleja kohustused sätestatud direktiiviga 95/46/EÜ. Kuid tulenevalt IKT kiirele arengule tekkis aja jooksul vaja uue õigusliku raamistiku järgi, mis oleks vastavuses omakorda tehnoloogilise reaalsusega, sest aastal 1995 vastu võetud direktiiv ei olnud enam ajakohane. Selle tulemusena võeti vastu Euroopa Parlamendi ja Nõukogu Määruse füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (Isikuandmete Kaitse Üldmäärus), mis hakkab kehtima aastal 2018.

Kuigi eelnenud direktiivi kesksed mõisted, kui ka kontseptsioon on jäänud samaks, kätkeb üldmäärus endas täiesti uut eesmärki. Andmekaitsedirektiivi rakendamise hindamine näitas seda, et direktiivi ülevõtmisel liikmesriikidele jäetud vormi ja meetodite valik ning riigiti erinevad ühiskondlikud ja õiguslikud arusaamad on endaga kaasa toonud direktiivi oluliselt erineva käsitluse, mille tõttu on tekkinud fragmentatsiooni tõttu oluliselt suurem administatiivne koorem, mille tõttu on seekord tegemist otsekohaldatava ja õiguslikult siduva määrusega, mis plaani päraselt peaks tugevdama andmesubjekti fundamentaalset õigust isikuandmete kaitsele ning privaatsusele.

Selleks, et suurendada andmesubjekti õigus senisest on üldmäärusesse sisse toodud vastavalt uued põhimõtted nagu lõimitud ning vaikimisi andmekaitse, täiendatud on andmetöötleja vastutuse kohta käivat peatükki ning sisse on toodud õigus kustutamisele ning eraldiseisev läbipaistvuse printsiip.

Mobiilse tervishoiu teemat on seadusandja otseselt puudutanud Tegevusjuhendis, mis on uudne iseregulatiivne võimalus, mis annab võimaluse luua organisatsiooni sisese kontrollmehhanismi. Tegevusjuhendi eesmärgiks on luua konkreetsed, arusaadavad ning praktilise sisuga juhtnöörid, mille läbi on võimalik GDPR-is välja toodud põhimõtteid lihtsamalt kohandada ja otseselt seostada m-tervishoiu valdkonnaga. Tegevusjuhend on otseselt suunatud rakenduste arendajatele, see tähendab, et sellest võivad juhinduda nii üksikisikuid, organisatsioonid, kui ka ettevõtted, kes võimaldavad kas otse või läbi rakenduste poe terviseandmete töötlust. Seadusandja on otsustanud sellise fookuse kasuks, sest rakenduste programmeerijad ning pakkujad omavad suuremat kontrolli selle üle, millised ulatuses rakendused tegelevad andmetöötluse ning kogumisega. Selline lahendus on valitud seetõttu, et seaduslooja on aru saanud sellest, et uue üldmääruse vastuvõtmiselt ei pruugita veel lahendada kõiki õiguslike probleeme, mille tõttu on vastu võetud erimeetmed. Samuti on seadusloome protsess reeglina aeglane, mille tõttu ei ole tark vastu võtta ülimalt spetsiifilisi reegleid, mis võivad kiiresti aeguda. Tegevusjuhend pole küll õiguslikult siduv, kuid autori arvates on see siiski arvestades asjaolusid parimaks lahenduseks, samuti on seadusandja selle läbi panustanud otseselt m-tervishoiu arengusse.

Teise peatüki eesmärgiks on vaadata terviseandmete mõiste tähendust m-tervishoiu kontekstis. Nõrgaks kohaks on siinjuhul andmete eristamine, sest tegu võib olla toore ning kasutu informatsiooniga või tundliku terviseandmetega. Teatud andmed on küll seotud

kaudselt inimese tervisliku seisundiga, kuid on oma olemuselt täiesti sisutud. Teave päevas tarbitud kalorite kohta ei oma mingisugust kaalu traditsiooniliste terviseandmetega võrreldes, mille tõttu puudub vajadus rakendada karmimat reeglistikku.

Peatükis keskendutakse andmete hilisemale töötlusele läbi suurandmestiku ning pilvetehnoloogia kasutuse. Sellised uued tehnoloogiad ei ole vastavuses traditsiooniliste andmekaitse printsiipidega. Sellised tehnoloogiad on täielikult uuendanud andmetöötluse mõistet. Läbi suurandmestiku ning pilvetehnoloogia kasutuse on võimalik koguda andmeid esiteks tohutult suures koguses, väga kiiresti ning kombineerida vastavalt vajadusele, mis suurendab läbipaistmatuse probleemi. Lisaks sellele ei oma kasutaja enam kontrolli enda kohta väiva üle. Seda selletõttu, et kui kasutada näiteks pilvetehnoloogiat, siis samal pilvel on reeglina mitu kasutajat, mis tähendab seda, et mitmed inimesed pääsevad sinna riputatud teabele ligi. Samuti on teenuse pakkujal võimalik järgida ning kontrollida andmete liikumist pilves. Selliste lahenduste kasutamisel on ülimalt tähtis see, et järgitakse andmekaitselisi põhimõtteid, mida tuleks vastavalt ka edasi arendada.

Kolmandas peatükis jõuab autor järeldusele, et kuigi m-tervishoiu näol on tegemist valdkonnaga, mis oma uudsuse näol toob kaasa mõningaid raskusi andmekaitseõiguse kohaldamisel tagavad kõik olemasolevad printsiibid siiski piisava kaitse.

Esiteks on olemas tugev põhiseaduslik alus, mille kohaselt on seadusandjal kohustus efektiivne kaitse andmekaitse vallas. Ning läbi üldmääruse analüüsi selgub, et oluliselt on tugevdatud üksikisikute õiguste kaitset. Seda arvamust toetavad uuenduslike printsiipide sisse toomine seadusesse ning samuti terviseandmete definitsiooni andmine.

Kõige olulisemaks uuenduseks on IKU artikkel 25 seoses andmekaitse vaikimisi valimisega ning lõimimisega. Lähtutakse põhimõttest, et infotehnoloogiaga seotud eluvaldkonnad on siiski läbipaistmatud, mis tähendab seda, et sisuliselt võimatu on süstemaatiliselt välja tuua vigu. Selle probleemi tasakaalustamiseks on sisse toodud põhimõtte, mille kohaselt peavad algseadistuses juba olemas olema maksimaalne andmekaitse ehk töötleja poolt on automaatselt läbi viidud parimad valikud. Lõimimine eeldab endas aga seda, et andmekaitsega peab tegelema juba algselt toote disainimise juures. Ettevõtted juba eelnevalt teevad kõik võimaliku selleks, et teenus või toode oleks võimalikult funktsionaalne privaatsust arvesse

võttes. Mis tähendab seda, et ettevõtted peavad üle vaatama oma senise käitumismalli ning kohandama end vastavalt seadusele.

Selleks, et andmesubjekti õigused oleksid hästi kaitstud on vajalik see, et andmekaitse reeglistikku on võimalik kohaldada ning jõustada praktikas. GDPR jõustub alles aastal 2018, selletõttu ei oska autor ette näha, mida tulevik toob, esialgse analüüsi põhjal näib, et tegemist on siiski piisavalt efektiivsete meetmetega. Autori seisukohal on hetkel eksisteeriv õiguslik raamistik rakendatav digitaalses maailmas.

Summary

Data protection framework in the field of m-health

Aet Veges

In author's thesis the strong relationship between ICT and data protection framework is revealed. Modern data protection is based on the technological revolution of the 70s. The use of smart devices have become an integral part of modern life, according to the statistics over half of the Estonian population owns a smart device. Smartphone user experience is built on the usage of different applications or apps that can provide a variety of services that operate by collecting and processing personal data. Mobile health (m-health) is a specific category of apps, it is a relatively new termin used to reference using mobile phone applications for health purposes.

The aim of this thesis was to analyse current and future data protection regulatsions to see if they apply in the field of m-health. The central question is does the data protection framework offer sufficient protection in the field of m-health. Although at the moment Directive 95/46 / EC is still in force, the authors thesis is primarly based on the new General Data Protection Directive (GDPR).

It is a complex and wide area due to the wide range of data that could fall under the category of health data. Due to the sensivity of the data that is used in m-health sector, strickter rules must be followed. But because the field of m-health is quite new, the application of data protection standards can be complicated. While m-health has many advantages as well as the potential to reform health sector as we kow it, the rights and freedoms of the individual should not suffer at its expense.

Authors thesis is based on different European Union data protection regulations as well as opinion papers from the Article 29 Working Party and European Data Protecton Supervisor as well as others. Due to the novelty of the field, academic literature on the topic is very limited,

this is why most sources are foreign and could be found on the Internet. However, few previous academical works as well as Juridica articles proves to be useful, because of the similar content relating to privacy and data protection in general. Thesis subsequently divided into three chapters.

n the first chapter the author gives an overview of the existing legal framework, as well as mapping central concepts regarding personal data and health data. Data protection has close ties with the right of privacy. An individual's right to privacy has been one of the most renowned law of the European Union, it is a pillar of modern society because it is directly linked to dignity. The European Convention of Human Righst article 8 provides a right to respect for private and family life, this is also stated in the article 7 of of the Charter of Fundamental Rights of the European Union. Though there is no direct link between the words private life and data protection, the European Commission, as well as European Court of Justice and European Court of Human Rights have concluded that the terms have a direct relationship, which makes it possible to derive one from the other. The Charter also establishes separately the right to data protection in article 8.

The central concept of data protection regulation is personal data and in accordance to the thesis health data. Personal data is defined as information relating to an identified or an identifiable natural person. It is a broad concept because potentially every kind of data can be personalized which is why it is impossible to give an exhaustive list. A separate category of personal data is health data which falls under special protection due to the fact that improper use of sensitive data is a bigger threat to individuals privacy.

Previously, the rights of the data subject and the controller obligations were regulated by Directive 95/46 / EC. However, due to the ICT rapid development, the need for a new legal framework arised resulting in the adoption of the General Data Protection Directive which will come in force in 2018. Although the central concepts of the previous directive have remained the same, the purpose of the regulation is quite different. The new regulation aims to harmonize the level of data protection within the EU, support innovation and to introduce more precise provisions in regard of the economy in order to respect the fundamental right to personal data protection more efficiently.

In order to increase the data subject's rights and provide a higher level of protection, the GDPR has introduced some new measures such as Privacy by Design and Privacy by Default, transparency principle, a new chapter concerning the controller and processor as well as the right to erasure.

Regarding to m-health the EU has has turned to a nontraditional measure of self regulation known as Code of Conduct on privacy for mHealth apps. Code of Conduct is intended to provide specific and comprehensible instructions on how to apply the data protection rules in the field of m-health. Code is specifically targeted towards app developers due to the fact that they can control software solutions to what extent it will access and process personal data. This ensures that mobile health apps have been properly developed in compliance to the GDPR. European legislators have realized that the new GDPR may not solve all legal problems thus the adoption of special measures is required. Legislative process is generally very slow, therefore it is not wise to adopt highly specific rules, which can quickly become outdated. Code, while not legally binding, is the best solution in author's opinion, also this way the EU directly contributes to the development of m-health.

Whole concept of m-health is built upon continious processing of health related data. The purpose of second chapter is to clarify the definition of health data in context to m-health. Certain data that is related indirectly to persons health status can be fundamentally meaningless. Information about calories consumed per day does not have any weight compared with traditional health data, therefore there is no need to implement a more stringent set of rules. There needs to be a distinction between well being data and traditional health data.

The author of this thesis will also focus on secondary use of health data by using big data and cloud computing. These new technologies are not in compliance with traditional data protection principles. Through the above-mentioned technologies it is possible to to collect enormous amounts of data very quickly that could be combinded as desired which makes the whole process extremely opaque. In addition to the lack of transparency, data subject has no control. For instance when using cloud technology, you can have multiple users on the same cloud, it means that many others have access to information, also the cloud service provider is able to control and track the movement of data on the Internet. As health data has an immense

value, it is very important to follow existing data protection principles as well as develop them further accordingly,

In the third chapter author concludes that while the m-health due to its novelty can lead to slight difficulty in applying data protection principles, all the existing rules are applicable and ensure adequate protection.

By analyzing the GDPR the author can conclude that the European Commission has significantly strengthened the protection of individual rights. Increased transparency in terms of obligating the data controller to explain easily and cleary to the data subject how exactly data is processed and why. Extended chapter on the rights and requirements of data controller which is particularly good solution considering how big data and cloud computing have blurred the lines between data subject and processor.

Although the right to erasure in authors opinion is difficult to apply in practice. Ideally it should strengthen the sense of individual rights and security. But the question arises can the service provider be able to get and delete all the information available given that data processing is very fast, large and difficult to follow.

The most important innovation is the Article 25 of the GDPR regarding data protection by default and design. The principle is derived from the idea that technology-related areas are opaque, which means that, essentially, it is impossible to identify systematically errors. To bring balance the notion of privacy must be taken to account while designing the product and the original configuration must include maximum data protection so automatically the best choice is carried out. It means that companies need to review their current behaviors and adapt themselves according to the law.

In order that the data subject's rights to be well protected its is necessary that the data protection rules can be applied and enforced in practice. GDPR will be in force in 2018, which means that the author cannot forsee what the future brings. But by doing a preliminary analysis the author can conclude that the current legal framework is sufficient to be implemented in the digital world.

Kasutatud kirjandus

Raamatud ning teadusartiklid

Bosco, F and Creemers,N and Ferraris,V and Gaugin,D and Koops.,BJ. (2015)Profiling Technologies and Fundamental Rights and Values: Regulatory Challenges and Perspectives from European Data Protection Authorities. Reforming European Data Protection Law. Dordrecht: Springer, 4.

Bygrave, L.A. (1998)Data Protection Pursuant to the Right to Privacy in Human Right Treaties.International Journal of Law and Information Technology, Vol.6, No.3, 255-259.

Cortez, N. (2014) The Mobile Health Revolution? UC Davis Law Review,Vol .4 , 1189.

Cukier, K and Mayer-Schoenberger, V. (2013) The Rise of Big Data. How It's Changing the Way We Think About the World. Foreign Affairs , Vol.92, No. 3, 28-29..

De Filippi, P an Belli, L. (2012) Law of the Cloud v Law of the Land: Challenges and Opportunities for Innovation. – European Journal of Law and Technology, nr 3, vol 2, 2.

De Hert, P.,Gutwirth,S. (2009) Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action. Reinventing Data Protection. Dordrecht: Springer Science.

Fink, U. (2014) Protection of privacy in the EU, individual rights and legal instruments. in Emerging Challenges in Privacy Law. Comparative perspectives. Cambridge: Cambridge University Press.

Frazee, J and Finley,M and Rohack, JJ. (2016) mHealth and Unregulated Data: Is This Farewell to Patient Privacy. Indiana Health Law Review, Vol. 13, No. 2, 384.

Hon, W.K and Kosta, E and Millard,C and Stefanatou, D. (2014) Cloud Accountability: The Likely Impact of the Proposed EU Data Protection Regulation. London: Queen Mary University of London, School of law, 14 - 15.

Ilus, T. (2005) Andmesubjekti osaluse põhimõte Euroopa Nõukogu konventsioonide ning Euroopa Inimõiguste kohtu lahendite valguses. Juridica, nr 8, 520.

Istepanian, R.S.H andLacal,J. (2003) Emerging mobile communication technologies for health: some imperative notes on m-health, in: Proceedings of the 25th Annual International Conference of the IEEE Engineering in Medicine and Biology Society, Vol. 2, 1414–1416.

Kokott, J and Sobotta, C. (2013) The distinction between privacy and data protection in the jurisprudence of the CJEU and the EctHR. International Data Privacy Law, Vol. 3, No. 4, 222.

Kranich, H. (2015) Ühiskonna (eba)normaalne areng ja inimõigused. Nimede kohtulahendites avalikustamise näide. Juridica, nr, 277-289.

Laffranque, J (2010) Eesti põhiseaduse ja Euroopa õiguse kooselu. Juridica, nr 3, 180-190.

Letsas,G. (2013) The ECHR as a living instrument: its meaning and legitimacy. In Constituting Europe. The European Court of Human Rights in a National, European and Global Context. Cambridge University Press: Cambridge .

Liiv, E. (2014) Kas eraisikul on õigus unustusele Internetis? Juridica, nr 9, 643-651.

Lynskey, O (2014) Deconstruction Data Protection: The „Added-Value" of a Right to Data Protection in the EU Legal Order. International & Comparative Law Quarterly, vol.63, no.3, 597.

Lynskey,O. (2010) Deconstruction Data Protection: The „Added-Value" of a Right to Data Protection in the EU Legal Order. Iinternational & Comparative Law Quarterly, Vol. 63, No. 3, 570.

Mantovani, E and Antokol, J and Hoekstra, M and Nouwt, S and Schutte,N and Zilgalvis,P and Castro Gómez-Valadés, J-P and Prettner,C. (2011) Data Protection and Privacy: (In)visibilities and Infrastructures. Law, Governance and Technology Series, Vol. 1, 88.

Mantovani,E and Quinn,P. (2014) mHealth and data protection – the letter and the spirit of consent legal requirements. International Review of Law, Computers and Technology, Vol. 28, no.2, 222-236

Maruste, R. (2010) Põhiõiguste harta Euroopa põhiseaduslikus lepingus. Juridica, nr 10, 655-660.

Matjus, M ja Haamer, M. (2014) E-tervis. Millistel tingimustel võib edastada patsiendi terviseandmeid Euroopa Liidu teise liikmesriiki? Juridica, nr 5, 361-373.

Rest van, J and Boonstra,D and Everts,M and Rijn van, M and Paassen van, R. (2012) Designing Privacy by Design. Lecture Notes on Computer Science: Privacy Technologies and Policy, 52-77.

Robinson, N and Graux, H and Botterman, M. and Valeri, L. (2009) Review of the European Data Protection Directive. Cambridge: RAND, 28.

Senden, L. (2005) Soft-law, self-regulation and co-regulation in European law: Where Do They Meet? Electronic Journal of Comparative Law, Vol. 9, No.1, lk 1-2.

Stark, P. (2014) Privacy, Big Data, and the Public Good: Frameworks for Engagement. Cambridge; Cambridge University Press, vol.70, no.1, 5-43.

Zanfir, G. (2012) The right to Data portability in the context of the EU data protection reform. International Data , Privacy Law, Vol. 2, No. 3, 156.

Tene, O and Polonetsky, J. (2012) Privacy in the age of big data: a time for big decisions. Stanford Law Review Online, Vol. 64, 16.

Tikk, E ja Nõmper,A. (2007) Informatsuoon ja õigus. Tallinn: Juura, 36-38

Tupay, P-K.ja Mikiver, M. (2015)E-riik ja põhiõigused. Juridica, nr 3, 163-176.

Van der Sloot, B. (2014) Do data protection rules protect the individual and should they? An assessment of the proposed General Data Protection Regulation. International Data Privacy Law, Vol. 4,No. 4, 309.

Velsen van, L and Beaujean, DJ and Gemert-Pijen van, JE. (2013) Why mobile health app overload drives us crazy, and how to restore the sanity. BMC Medical Informatics and Decision Making, Vol. 1, 13.

Wetherall, D and Choffnes, D and Greenstein, B and Han, S and Hornyack, P and J,Jung and Schecter, S and Wang, X. (2011) Privacy Revelations for Web and Mobile Apps. University of Washington; Intel Labs, 1.

Elektroonilised allikad

Andmekaitse Inspektsioon. (2014) 2014. a interneti rehitsemise päeva seire kokkuvõte.- Kättesaadav: http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/Interneti%20seire%20p%C3%A4eva%20kokkuv%C3%B5te%20%28l%C3%B5plikI%29.pdf, 20.aprill 2017.

Andmekaitse Inspektsioon. (2014) Pilvandmetöötlus.- Kättesaadav: http://www.aki.ee/et/pilvandmetootlus, 13.aprill 2017.

Andmekaitse Inspektsioon. (2017) Suurandmed ja privaatsus ,Juhendmaterjal organisatsioonidele.- Kättesaadav: http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/suurandmed_ja_privaatsus.pdf, 16.veebruar 2017.

Andmekaitse Inspektsioon. (2017) Vaikimisi ja lõimitud andmekaitse.- Kättesaadav: http://www.aki.ee/et/andmekaitse-reform/vaikimisi-ja-loimitud-andmekaitse, 12.aprill 2017.

Artikkel 29 alusel asutatud andmekaitse töörühm. (2000) Advice Paper on Special Categories of Data (sensitive data).- Kättesaadav: http://www.europarl.europa.eu/charter/pdf/text_en.pdf

Artikkel 29 alusel asutatud andmekaitse töörühm. (2007) Arvamus 4/2007 isikuandmete mõiste kohta.- Kättesaadav: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_et.pdf, 04.aprill 2017.

Artikkli 29 alusel asutatud andmekaitse töörühm. (2013) Arvamus 02/2013 nutiseadmete rakenduste kohta.- Kättesaadav: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_et.pdf, 10.november 2016.

Artikli 29 alusel asutatud andmekaitse töörühm. (2009) Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data. The future of privacy.- Kättesaadav: http://ec.europa.eu/justice/data-

protection/article-29/documentation/opinion-recommendation/files/2009/wp168_en.pdf, 13.veebruar 2017.

Artikli 29 alusel asutatud andmekaitse töörühm. (2011) Annex - health data in apps and devices.- Kättesaadav: http://ec.europa.eu/justice/data-protection/article-29/documentation/other document/files/2015/20150205_letter_art29wp_ec_health_data_after_plenary_annex_en.pdf, 11.jaanuar 2017.

Artikli 29 alusel asutatud andmekaitse töörühm. (2012) Working Document 01/2012 on epSOS.- Kättesaadav: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp189_en.pdf, 11.jaanuar 2017.

Artikli 29 alusel loodud andmekaitse töögrupp. (2014) Statement on Statement of the WP29 on the impact of the development of big data on the protection of individuals with regard to the processing of their personal data in the EU.- Kättesaadav: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp221_en.pdf, 13.aprill 2017.

Boyles, J.L and Smith, A. and Madden, M. (2012(Privacy and Data Management on Mobile Devices-. Kättesaadav: http://www.pewinternet.org/2012/09/05/privacy-and-data-management-on-mobile-devices/, 10.november 2016.

Cavoukian, A. (2009) Privacy by Design. The 7 Foundational Principles.-Kättesaadav: https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf, 03.märts 2017.

Commission of the European Communities. (2003) European Comission report. First report on the implementation of the Data Protection Directive (95/46/EC).- Kättesaadav: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2003:0265:FIN:EN:PDF, 03.detsember 2016.

EMOR. (2014) Nutiseadmete kasutajate turvateadlikkuse ja turvalise käitumise uuring.- Kättesaadav: https://www.ria.ee/public/Programm/Nutiseadmete_kasutajate_turvateadlikkuse_ja_turvalise_kaitumise_uuring_ARUANNE_2014_LUHI2.pdf, 10.jaanuar 2016.

Euroopa Andmekaitse Inspektor. (2015) Euroopa andmekaitseinspektori arvamuse kokkuvõte teemal „Mobiilne tervishoid: tehnoloogilise innovatsiooni ühitamine andmekaitsega".- Kättesaadav: https://edps.europa.eu/sites/edp/files/publication/15-05-21_mhealth_summary_et.pdf, 16.aprill 2017.

Euroopa Andmekaitseinspektor. (2016) „Suurandmetega kaasnevad probleemid: üleskutse läbipaistvusele, kasutajate kontrollile ja andmekaitsele disaini ning aruandekohustuse abil".- Kättesaadav: https://edps.europa.eu/sites/edp/files/publication/16-02-20_challenges_of_big_data_et.pdf, 14.jaanuar 2017.

Euroopa Komisjon. (2010) Euroopa Komisjoni teatis Euroopa Parlamendile, Euroopa Majandus- ning Sotsiaalkomiteele ning Regionaal komiteel. Euroopa Digitaalne Majanduskava .- Kättesaadav: http://eur-lex.europa.eu/legal-content/et/ALL/?uri=CELEX:52010DC0245R(01), 18.aprill 2017.

Euroopa Komisjon. (2010) Komisjoni teatis Euroopa Parlamendile,Nõukogule, Majandus- ja Sotsiaalkomiteele ning Regiooni Komiteele. Terviklik lähenemisviis isikuandmete kaitsele Euroopa Liidus.- Kättesaadav: http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_et.pdf, 23.jaanuar 2017.

Euroopa Komisjon. (2016) Kuidas kohandatakse ELi reformiga andmekaitse-eeskirju uue tehnoloogilise arenguga?.- Kättesaadav: http://ec.europa.eu/newsroom/document.cfm?doc_id=41579, 17.detsember 2016.

Euroopa Liidu Põhiõiguste Amet. (2013) Juurdepääs andmekaitse õiguskaitsevahenditele Euroopa Liidu liikmesriikides. Kokkuvõte.- Kättesaadav: http://bookshop.europa.eu/et/juurdepaeaes-andmekaitse-iguskaitsevahenditele-euroopa-liidu-liikmesriikides-pbTK0113752/downloads/TK-01-13-752-ET-C/TK0113752ETC_002.pdf?FileName=TK0113752ETC_002.pdf&SKU=TK0113752ETC_PDF&CatalogueNumber=TK-01-13-752-ET-C, 12.oktoober 2016.

Euroopa Liidu Põhiõiguste Amet. (2014) Twelve operational fundamental rights considerations for law enforcement when processing Passenger Name Record (PNR) data.- Kättesaadav:

https://www.google.ee/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwitrO2N6s_TAhWjKJoKHUrvA5IQFgglMAA&url=https%3A%2F%2Ffra.europa.eu%2Fsites%2Fdefault%2Ffiles%2Ffra-2014-fundamental-rights-considerations-pnr-data-en.pdf&usg=AFQjCNFrhjNS8_oxAv0aGHBl2eGCSFD6VQ&sig2=dFJT8JP68nVXHvPCX_nlFw, 23.jaanuar 2017.

Euroopa Ülemkogu. (2014) Järeldused.- Kättesaadav: . http://www.riigikogu.ee/?op=emsplain&page=pub_file&file_id=5e49dedb-09a1-479b-acbf-09ef47bf0897&.pdf, 18.aprill 2017.

European Comission. (2016) Draft Code of Conduct on privacy for mobile health applications.- Kättesaadav: http://ec.europa.eu/newsroom/dae/document.cfm?action=display&doc_id=16125, 18.aprill 2017.

European Commission. (2012) Commission Staff Working Paper. Impact Assesment.- Kättesaadav:. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=SEC:2012:0072:FIN:EN:PDF, 17.detsember 2016.

European Commission. (2012) eHealth Action Plan 2012-2020: Innovative healthcare for the 21st century.- Kättesaadav: https://ec.europa.eu/digital-single-market/en/news/ehealth-action-plan-2012-2020-innovative-healthcare-21st-century, 12.veebruar 2017.

European Data Protection Supervisor. (2015) Opinion 1/2015 Mobile Health. Reconciling technological innovation with data protection.-Kättesaadav: https://edps.europa.eu/sites/edp/files/publication/15-05-21_mhealth_en_0.pdf, 11.jaanuar 2017.

European Digital Rights. (2013) An introduction to data protection.- Kättesaadav: https://edri.org/files/paper06_datap.pdf, 12.aprill 2017.

GSMA. (2012) mHealth and the EU regulatory framework for medical devices.- Kättesaadav: ://www.gsma.com/connectedliving/wp-content/uploads/2012/03/mHealth_Regulatory_medicaldevices_10_12.pdf, 16.aprill 2017.

http://ec.europa.eu/justice/data-protection/article-29/documentation/otherdocument/files/2011/2011_04_20_letter_artwp_mme_le_bail_directive_9546ec_annex1_en.pdf , 20.jaanuar 2017.

Hustinix, P. (2013) EU Data Protection Law - Current State and Future Perspectives.- Kättesaadav: http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/Hustingx.pdf, 07.jaanuar 2017.

IHS Markit. (2013) The World Market for Sports & Fitness Monitors—2013 Edition.- Kättesaadav: http://news.ihsmarkit.com/press-release/design-supply-chain/sports-and-fitness-app-market-expand-more-60-percent-five-years, 03.november 2016.

intelligence, machine learning and data protection.- Kättesaadav: https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf, 03.jaanuar 2017.

International Commissioner's Office. (2016) Big data, artificial

PwC Luxembourg. (2014) European Hospital Survey: Benchmarking Deployment of eHealth Services (2012–2013.- Kättesaadav: http://ipts.jrc.ec.europa.eu/publications/pub.cfm?id=7060 21.oktoober 2016.

Reding,V. (2012) The EU Data Protection Reform 2012: Safeguarding Privacy in a Connected World. Speech.- Kättesaadav: http://europa.eu/rapid/press-release_SPEECH-11-183_en.htm, 04.veebruar 2017.

Research2Guidance. (2013) Mobile health app market report 2013–2017: The commercialization of mHealth. Research2Guidance.- Kättesaadav: http://www.researchandmarkets.com/reports/2497392/mobile_health_app_market_report_201 32017_the, 03.november 2016.

Ruback, T. (2015) A Brief Look at Self-Regulation and European Data Protection.- Kättesaadav: https://iapp.org/news/a/a-brief-look-at-self-regulation-and-european-data-protection/, 12.veebruar 2017.

Silber, D. (2003) The Case for eHealth.- Kättesaadav: . http://www.denisesilber.com/files/case_for_ehealth03.pdf, 23. November 2016.

World Health Organization. (2011) mHealth - New horizons for health through mobile technologies.- Kättesaadav: http://www.who.int/goe/publications/goe_mhealth_web.pdf, 12.oktoober 2016.

Soosaar, S. (2004) Inimese autonoomia ja informeeritud nõusolek kui protsessid.- Kättesaadav: http://andressoosaar.planet.ee/autonoomia%20&%20consent%20kui%20protsessid.pdf, 16.märts 2017.

Kohtulahendid

Euroopa Inimõiguste Kohtu otsus. 25.veebruar 2009, kohtuasjades 36919/02 ja 23373/03

Euroopa Kohtu otsus. 6.november 2003, kohtuasjas C-101/01

Euroopa Kohtu otsus. 13.mai 2014, kohtuasjas C-131/12

Euroopa Kohtu otsus. 5.juuli 2011, kohtuasjas F-46/09

Euroopa Liidu õigusaktid

Euroopa Liidu Põhiõiguste Harta. 30.märts, 2010.

Euroopa Parlamendi ja Nõukogu 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), 27. aprill 2016.

Inimõiguste ja põhivabaduste kaitse konventsioon. 4. november 1950.

Inimõiguste Ülddeklaratsioon. 10. detsember 1948.