

INIMÕIGUSED, INFOÜHISKOND JA EESTI: ESIALGNE KAARDISTUS

AUTORID: KARI KÄSPER, LIINA RAJAVEER
EESTI INIMÕIGUSTE KESKUS 2019



Kaardistust rahastati Euroopa Põhivabaduste Ühenduse projektist “Liikmete digitaalne võimestamine,” mida omakorda rahastas Ford Foundation. Aruanne ei väljenda selle rahastajate seisukohti.

Kaanefoto: Bernard Hermant, Unsplash

Kaardistus on litsenseeritud Creative Commons Attribution-NonCommercial 4.0 International License alusel.

Vaata lähemalt:
<http://creativecommons.org/licenses/by-nc/4.0/>

SISUKORD

3	Sissejuhatus
5	Teemade kaardistus
7	Olukord Eestis
13	TEEMA 1 - Profileerimine ja riik
18	TEEMA 2 - Isikuandmete kaitse üldmääruse (GDPR) rakendamine
22	TEEMA 3 - Väljendusvabadus internetis
25	Ideed teadlikkuse tõstmiseks
26	Eesti Inimõiguste keskus ja digitaalsed õigused

SISSEJUHATUS

Eesti on üle maailma tuntud kui digitaalühiskond. Eesti puhul on tõesti tegemist e-valitsemise valdkonnas ühe eesrindlikuma riigiga maailmas, kuid maine on tegelikkusest mõnevõrra kaugemal ees ning senine “move fast and break things”-lähenedmine ei pruugi enam kohane olla. Maailmas tunnistatakse üha enam infotehnoloogiaga seotud riske ja väljakutseid inimõigustele, eriti pärast Ameerika Ühendriikide vilepuhaja Edward Snowdeni paljastusi luureagentuuride lausjälituse kohta ning Cambridge Analytica skandaali, mis puudutas Facebooki mikrosihistuse kasutamist demokraatlike otsuste mõjutamiseks (Brexiti referendum Ühendkuningriigis, valimised USAs ja mujal). Üha enam on samuti levinud küpsem arusaam, et innovatsioon on oma olemuselt poliitiliste valikute küsimus ning et tehnoloogia arengut saab tarkade poliitikate ja seadustega suunata.

Tehnoloogia ei ole üheselt positiivse, negatiivse ega neutraalse mõjuga. Samamoodi on infotehnoloogia mõjuga inimõigustele. Uued tehnoloogiad nagu tehisintellekt või sotsiaalmeedia on hea võimalus inimõiguste rikkumisi vähendada, välistades näiteks inimlike eelarvamuste osakaalu otsuste tegemisel või andes võimaluse inimõiguste rikkumistest kiiresti ja lihtsalt teada anda. Levivad ka privaatsust kindlustavad tehnoloogiad ja krüpteerimine ning anonümiseerimine, mis võimaldavad ini-

mestel oma õigusi paremini kaitsta. Teisalt ohustab inimõigusi kiire infotehnoloogia lahenduste kasutuselevõtt, mis võib olemasolevaid inimõigusi rikkumisi süvendada ja lihtsamaks teha (näiteks kui jätta tehisintellekti puhul arvestamata ajaloolistes andmetes sisalduv ebaõiglus või võimaldada vaenu õhutamist). Igasugune laialdane isikuandmete töötlemine kujutab endast omakorda ka potentsiaalselt tugevat riivet eraelu puutumatu- sele ning õigusele isikuandmete kaitsele. Seetõttu on oluline, et enne infotehnoloogiliste lahenduste kasutuselevõttu oleks hinnatud nende võimalikke mõjusid inimõigustele ning negatiivsed mõjud maandatud.

Eesti Inimõiguste Keskus uuris sügisel 2019 tehnoloogia mõju inimõigustele Eestis. Tegemist on esialgse kaardistusega, mille eesmärk oli saada parem arusaam digitaalvaldkonna ja inimõiguste teemadest, ohtudest ja võimalustest Eestis, ülevaade olulistest tegijatest nii inimeste kui institutsioonide mõttes, luua teadlikkus Eesti Inimõiguste Keskusest kui inimõiguste valdkonna eestvedajast ja teadmuskeskusest, ning saada põhjalikum arusaam kolmest teemast.

Kaardistuse raames töötasime läbi olulised dokumendid, ent peamine rõhk oli rühmaaruteludel ning individuaalintervjuudel.

Kohtusime inimestega, kes puutuvad digitaalvaldkonna teemadega kokku nii erasektoris advokaatide või ettevõtjatena, avalikus sektoris poliitikakujundamise või järelevalve eest vastutavate ametnikena. Samuti andsid oma panuse vabakonna aktivistid ning teadlased ja üks ajakirjanik. Kokku kohtusime 19 inimesega, kes andsid oma vaate teemale poolstuktureeritud intervjuude käigus. Käesolev kaardistus põhineb nii nende intervjuude kokkuvõtetel kui ka eraldiseisval uurimistööl.

**TEEMADE
KAARDISTUS**

TEEMADE KAARDISTUS

Pakkusime harjutusena välja hulga teemasid, mida eksperdid hindasid relevantsuse järgi. Kõige enam peeti oluliseks isikuandmete kaitse üldmäärusega seotut: selle korrektset rakendamist. Samuti peeti probleemseks profileerimist ja tehisintellektil põhinevaid lahendusi avalikus sektoris. Olulise teemana tõusis esile ka väljendusvabadus internetis.

Teise grupi moodustasid teemad nagu lausjälitus ja sellega seonduv side- ja muude andmete kasutamine julgeolekuasutuste poolt. Samuti erasektoris levinud profileerimine. Eraldi märgiti ka näotuvastust kui eriti inimõigusi riivavat tehnoloogiat. Samuti toodi läbivalt esile digitaalset lõhet ja sellest põhjustatud ilmajätust, millega Eestis pole piisavalt tegeletud.

Vähem peeti relevantseks eraldi keskendumist targa linna lahendustele, tarkadele piirivalvelahendustele, droonide kasutamisele jälituseks, julgeolekuasutuste piiriülesele koostööle. Nende teemade osas on Eestis tõenäoselt veel vähe teadmisi, või on need liiga kitsad. Võimalik, et neid peeti ka juba kaetuks laiemate teemadega. Masinkäitumise temaatika võib seada universaalsuse ja kohalikud tavad ja seadused konflikti.

Kindlasti ei saa seda teemade kaardistust pidada ammendavaks. Digitaalõiguste valdkond on kiiresti arenev ning uued teemad

võivad tekkida kiiresti ning ka kaduda. Samas võib täheldada, et digitaalõiguste valdkonnas tõusevad esile Eestis samad teemad, mis Euroopas ja mujal maailmas. Sellele lisanduvad Eesti e-valitsemise spetsiifikat puudutavad teemad, mida pole mujal veel kuigi palju proovitud, nagu näiteks profileerivad ja tehisintellekti kasutavad proaktiivsed või ettehoolitsevad avalikud teenused.

Huvitav on, et ohtu nähakse peamiselt riigi tegevuses, erasektori inimõigusi ohustav tegevus aruteludes palju mainimist ei leidnud. See võib olla seotud sellega, et inimõigusi ohustavad suurte korporatsioonide ülemaailmsed platvormid nagu Google, Facebook, YouTube ja Twitter, mis pole Eestis eraldi kanda kinnitanud ning kellest ehk ei peeta jõudu üle käivaks. Kohalikud ettevõtted on oma tegevuses suhteliselt märkamatud ning nende põhjustatud ohtusid ei osata nii konkreetselt ette näha.

**OLUKORD
EESTIS**

“Eesti digivaldkonna regulatsioon on see komme, et reguleeritakse asju selleks, et riigil oleks mugav - pannakse kübertempel peale, et inimene kohe unustaks ära, millega tegu.”

–fookusgrupis osalenud ekspert

OLUKORD EESTIS

AVALIKUD ARUTELUD JA TEADLIKKUS

Eestis on üpris vähe asjatundlikku avalikku arutelu tehnoloogia mõjudest inimõigustele. Selle põhjused on mitmetahulised: küsimused on tehnilist laadi ja keerulised ning pole ka eriti pingutatud, et teemasid selgitada ja paremini käsitleda. Valdkond on suhteliselt uus ja kiirelt arenev, mistõttu on vähe eksperte ning teisi, kes suudaksid teemat avalikkusele arusaadavalt käsitleda.

Laiem avalikkus ei ole Eestis üldiselt teadlik erinevatest digitaallõiguste teemadest. Seega võib väita, et teema käsitlust iseloomustab paljude jaoks ilmajaetus, mis on põhjustatud digitaalsest lõhest. Paljudel Eesti inimestel pole piisavalt teadmisi ja oskusi tehniliste lahenduste osas. Probleemaatilisem on, et paljudel puudub ka sõnavara ja arusaamine, et üldse teemal kaasa rääkida. Seetõttu on lihtsad ka levima kuulujutud ja hirmud, aga tekiavad ka küsimused valdkonnas tehtud otsuste demokraatliku legitiimsuse kohta.

Omaette suur probleem on see, et infotehnoloogilised lahendused teevad elu lihtsamaks sageli neil, kes pole ise haavatates rühmades. Rohkem tähelepanu tuleks juhtida sellele, kuidas IT-lahendusi luua nii, et need jõuaksid paremini haavatavate rühmadeni.

Inimesed ei suuda teadmatuse tõttu oma õigusi kaitsta ega mõista sageli oma inimõiguste väärtust ja vajadust internetis. Sagedasti lähtutakse internetis ekslikust arusaamast, et “mul pole ju midagi varjata”. Privaatsust ei peeta digikeskkonnas isegi sobilikuks nõuda.

Digiõiguste teemadest ei räägita sageli inimõiguste raamistikus, vaid pigem on raamistuseks muu, näiteks küberturvalisus. See ei pruugi olla iseenesest halb, kui küberturvalisusest rääkides üksikisiku õigused olulisel kohal on. Sellises kontekstis võivad julgeolekuasutused olla ka isikuandmete kaitse mõttes liitlased, kui rõhutada ohtu, mida isikuandmete liiga lai kättesaadavus võib kujutada. Üksikisikute inimõigusi digitaalmaailmas kajastatakse mõnikord negatiivses kontekstis, näiteks andmelekete puhul.

Samuti ei täida oma tavapärasest rolli ajakirjandus, sageli seetõttu, et vähe on ajakirjanikke, kes valdkonnas orienteeruvad. Isikuandmete kaitse ja privaatsuse teemadel võib olla ajakirjandusel ka huvi, et kaitse oleks võimalikult väike. Teisalt on tehnoloogiaajakirjanikud on sageli ise ITentusiastid, mistõttu ei pruugi neid huvitada käsitlused, mis nende meelest seavad tehnoloogia arengule piiranguid. Isikuandmete kaitse üldmääruse jõustumisel kasutas kohati erasektor teadmatust ära, et levi-
tada hirmu ja segadust ning seeläbi müüa koolitusi ning tooteid.

Tegemist on nõiaringiga: poliitikute seas eriti digitaalvaldkonnas inimõiguste teemadele toetust ei avaldata, see pole häälemagnet, sest rahvas ei ole eriti teadlik ega huvitatud. See omakorda tähendab, et olukord ei muutu paremaks ning pole poliitikuid-ar-

“Kui digitaalne maailm alguse sai, siis see algas hästi hiilimisi: oli üks meiliaadress ja muud polnudki. Ja siis järsku plahvatuslikult see suurenes ja see oli järsku nii võõras, et polnud võimalik sellega rahulikult kohaneda.”

–fookusgrupis osalenud ekspert

vamusliidreid, kes teemasid selgitaksid. Eestis usaldatakse avalikke asutusi suurel määral, mistõttu ei usuta, et tehnoloogia valdkonnas võivad need inimõigusi ohustada.

Üks ekspert juhtis tähelepanu ka USA ja Euroopa erinevustele. Kui USA meedias käib üpris aktiivne diskussioon digitaalvaldkonna mõju osas inimõigustele, siis Euroopas seda eriti ei ole. Selle põhjuseks võib olla USA palju suurem rohujuure tasandi aktivism nendes küsimustes.

Oma rolli võib mängida ka ajalooline taak. Nõukogude Eestis ei austatud inimõigusi, sh õigust eraelu puutumatusse. Vastupidi: levinud oli jälitamine ning võimud kutsusid üles teisitimõtlejaid üles andma. Seda, et inimõigusi võiks ohustada ka iseseisev ja demokraatlik Eesti riik või veel vähem eraettevõtted, ei peeta kuigi tõenäoliseks. Väikeriigi puhul on arusaam eraelust erinev võrreldes suuremate riikidega, kus anonüümsust rohkem.

HEAD ALGATUSED INIMÕIGUSTE KAITSEKS

Mitmed eksperdid tõid esile **andmejälgija**, mis võimaldab inimesel riigiportaalis näha, kes tema andmeid on vaadanud. Erinevalt paberdokumendist, mille vaatamisel taolist jälge tavaliselt ei teki. Samas leiti, et selle rakendamine erinevates riigi andmebaasides on erinev ning info andmete vaataja kohta on liiga napp: näiteks on sageli puudu võimalus lisada põhjendus, miks isikuandmeid vaadati. Lisaks ei ole vaid andmete jälgitavus iseenesest piisav õigustus isikuandmete koguma hakkamiseks. On ka olukordi, kus isikuandmeid ei peaks üldse koguma.

Samuti toodi välja avalike teenuste ja info **ligipääsetavus** veebides, mis võimestab seni kõrvalejätuid ning vähemkindlustatud, samuti inimesi, kellel on puue. E-teenuste kasutamisel säästetud raha võimaldab väiksemat riigilõivu riigiga seotud toimingute osas, mis suurendab teenuste kättesaadavust.

Hea näitena võib tuua ka **krüptopeod**, mille käigus inimesed õpivad, kuidas oma andmeid kaitsta: krüpteerida faile, brausida internetis jälitamata, õppida tugevaid parooli looma ja nii edasi.

Digiriik on kaasa toonud ka suurema läbipaistvuse, mis aitab ennetada ja avastada võimalikku korruptsiooni ning tagada reeglite ühetaolise kohaldamise.

EESTVEDAJAD JA TEGIJAD

Ekspertid ei osanud hästi välja tuua inimesi või institutsioone, kes võiks või peaks inimõiguste ja infotehnoloogia valdkonnaga tegelema: teadlikkust tõstma või inimesi kaitsma. Oma seadusest tulenev roll on **Õiguskantsleril** ning **Andmekaitse Inspektsioonil**. Riigisektorist toodi välja näiteks **õigusloomejuhtide ümarlaud**, kus sageli tõuseb debatt tehnootimistide ja konservatiivide vahel. Ministeeriumitest puutuvad teemadega kokku tihedamalt Majandus- ja Kommunikatsiooni-ministeerium ning Justiitsministeerium.

Ettevõtete rolli peeti seni üldiselt tagasihoidlikuks, sest Eesti tehnoloogiaettevõtted ei tähtsusta üldiselt eetika või inimõiguste küsimusi. Siin on võimalusi luua majanduslikke motivaatoreid

“Riigile oleks hea, kui oleks partner, kes juhib tähelepanu diskrimineerimisele, profileerimisele, algoritmikriitikale.”

–fookusgrupis osalenud ekspert

“Andmetega tegelemine on uus sotsiaalne kord. Üks, millest ma ise tunnen puudust, on kolmanda sektori andmeaktivism – inimesed, kes kasutavad avaandmeid, teevad samu prognoose, mida teevad teadlased ja pakuvad ühiskonnale mingeid lahendusi.”

–fookusgrupis osalenud ekspert

(uued ärivõimalused, parem maine, tõhusam järelevalve), et nad võtaksid inimõiguste küsimusi tõsisemalt. Erasektor näitab initsiatiivi alles siis, kui teemaga tegelemata jätmine on nende jaoks “valu”. Erasektorit peeti samas oluliseks viisiks, kuidas jõuda nende teemadega üksikisikuteni (kliendid, töötajad).

Oluliseks peeti palju tihedamat ja laiapõhjalisemat **koostööd** AKI, riigiasutuste ja vabaihenduste vahel, et vajakajäämistega tegeleda.

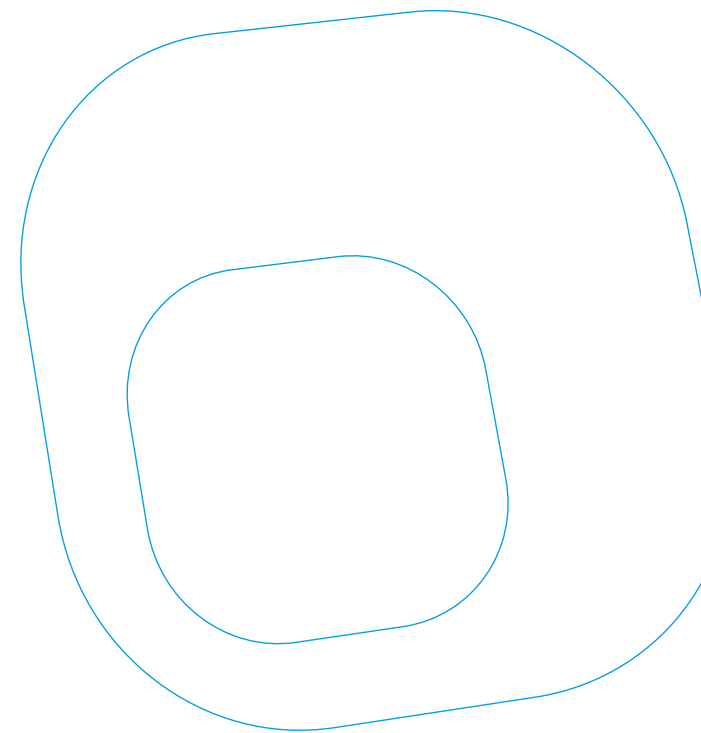
REGULATSIOONI ROLL

Pea kõik eksperdid leidsid, et täiendavat regulatsiooni pole vaja ning soovisid õigusrahu. Rõhutati, et pigem tuleks tegeleda konkreetsete seaduslünkadega, mis praktika käigus avalduvad. Osa eksperte tõi välja ka selle, et seadused valdkonnas on kohati vasturääkivad, mis võimaldab mitmetitõlgendavusi. Ühtlustada tuleks ka definitsioone, mida erinevates õigusaktides kasutatakse. Isikuandmete kaitse üldmäärust on vaja juurutada ning tagada selle tegelik ja tõhus toimimine. Peeti oluliseks uuendada sideandmete säilitamise ja kasutamise regulatsiooni.

Uute seaduste asemel on vajadus eetiliste raamistike ja üldpõhimõtete järgi, millega saaks tehnoloogiate kasutuselevõtul arvestada. Sageli on need juba olemas näiteks põhiõiguste kataloogi näol Põhiseaduses ning muude õigusaktide näol, aga neid ei osata rakendada tehnoloogia valdkonnas. Hea näitena nimetati Justiitsministeeriumi initsiatiivi vastutustundliku andmetötluse põhimõtete väljatöötamisel.

VABAÜHENDUSTE ROLL

Vabaühenduste rolli nähti eelkõige vajakajäämistele tähelepanu juhtijatena, kes küsivad infot erinevate temade kohta, kaevavad neid välja ning toovad avalikkuse ette. Samuti võiks vabaühendused olla partneriks riigile ja erasektorile. Lisaks leiti, et vabakond võiks rohkem vedada kvaliteetset ning teaduspõhist 7 Riigile oleks hea, kui oleks partner, kes juhib tähelepanu diskrimineerimisele, profileerimisele, algoritmikriitikale. –fookusgrupis osalenud ekspert diskussiooni. Täna ei nähta Eesti vabakonnas palju aktiviste, kes hästi orienteeruksid tehnoloogia ja andmete valdkonnas. Vabaühenduste roll võiks olla neid aktiviste ühendada ja mobiliseerida. Vabaühenduste rolli nähakse ka kaebuste esitamises, nõustamises ja kohtusse minekuga abistamises.



TEEMA 1

PROFILEERIMINE JA RIIK

“Jube lahe on teha mingi järjekordne register jne, selle asemel, et mõelda, äkki saab sama tulemuse saavutada teistmoodi.”

–fookusgrupis osalenud ekspert

TEEMA 1: PROFILEERIMINE JA RIIK

Riik kasutab üha enam inimeste profileerimist, ristkasutades erinevates riigi andmebaasides sisalduvaid andmeid. Seda tehakse erinevates olukordades, näiteks proaktiivsete teenuste puhul, poliitikakujundamist toetavaks andmeanalüüsiks, aga ka julgeoleku valdkonnas.

Proaktiivsed (ka ennetavad või ettehoolditsevad) teenused on uut tüüpi avalikud teenused, mida riigiasutus osutab omal initsiatiivil. See tähendab, et erinevalt traditsioonilistest avalikest teenustest, mille jaoks peab inimene pöörduma riigi poole, ei ole selliste teenuste puhul inimese tahteavaldus vajalik. Proaktiivsed teenused on väidetavalt kasulikud, sest need muudavad teenuste kasutamise inimese jaoks lihtsamaks ja ajasäästlikumaks. Need toimivad inimese jaoks “nähtamatult” ning käivituvad konkreetsete elusündmuste puhul (näiteks lapse sünd).

Teenuste korraldamise ja teabehalduse aluste kohaselt on proaktiivne teenus “otsene avalik teenus, mida asutus osutab oma initsiatiivil, isikute eeldataval tahtel ja riigi infosüsteemi kuuluvate andmekogude andmete alusel. Proaktiivne teenus osutatakse automaatselt või isiku nõusolekul.” Eestis proaktiivseid teenuseid praegu veel vähe, aga suundumus on neid üha rohkem kasutada, sealhulgas kasutades tehisintellekti abi.

Ühe esimese näitena alustas Sotsiaalkindlustusamet sünnitoe-
tuse automaatset pakkumist, mille puhul peavad vanemad vaid
pakkumise aktsepteerima. Proaktiivseid teenuseid plaanib käivi-
tada näiteks ka Töötukassa tööturuteenuste osas.

Suurandmete ja riigi andmebaasidega seonduvaid teemasid on
rohkem kui vaid proaktiivsetesse avalikesse teenustesse puutuv.
Eksperdid tõid välja näiteks vähese järelevalve riigi andme-ko-
gude üle, eriti kui neid kopeeritakse andmeaitadesse. On juhtunud
ka, et infotehnoloogised arendused, mis võimaldavad isiku-and-
meid kasutada, on tegemisel veel enne, kui õigusaktides see “le-
gaalseks muudetakse”.

Profileerimine julgeoleku valdkonnas on varjatud ning kontroll
nende teostatava jälituse üle seda olulisem

VÕIMALUSED JA OHUD

Inimõiguste mõttes on võivad profileerimise teel pakutavad teenu-
sed jõuda senisest enam inimesteni, kes varem ei olnud teadlikud
teenuse kasutamise võimalusest. See eeldab siiski süsteemi muut-
mist täisautomaatseks, viisil, mis ei eelda inimese nõusolekut või
ka aktsepteerimist. Kuigi Eestis ei ole olukorda eraldi analüüsitud,
on tõenäoline, et marginaliseeritud gruppide seas on avalike tee-
nuste kättesaadavus väiksem. Kui profileerimist kasutatakse vii-
sil, mis viib toetused ja riigi teenused enam nendeni, kes varem
erinevatel põhjustel neid vajasid, aga ilma jäetud oli, aitab see
kahtlemata kaasa tagada **õigust võrdsele kohtlemisele**.

“Kas riik peaks ütlema, et sa
peaksid ümber õppima, millal
vereproove andma. Kui proak-
tiivne peaks olema riik?”

–fookusgrupis osalenud ekspert

“IT lahendused võivad võimendada
ja teha olemasolevad probleemid
struktuurseteks.”

–fookusgrupis osalenud ekspert

Samas tekib iga uue andmekogu puhul oht inimese **õigusele era-elu puutumatus** ning **õigusele isiku-andmete kaitsele**. Tekib küsimus, millistel tingimustel ja kas inimesel on õigus ka proaktiivseid teenuseid mitte saada. Ohtu satub inimese autonoomia ja valikuvabadus.

Õigust mitte olla diskrimineeritud võib samas profileerimine ka ohustada, kui kasutatakse andmed on ebatäpsed või ebatäielikud. Sageli unustatakse tehisintellekti alusel profileerimisel ära, et ajaloolised andmed võivad olla juba eelarvamuslikud, samuti võib programmeerija eelarvamusi sisaldada loodav algoritm.

LAHENDUSED JA SOOVITUSED

1. Luua isikuandmete kasutamise terviklahendus, kus kodanik näeb lihtsalt ja selgelt (visualiseerituna), millised riigi teenused tema isikuandmeid kasutavad ja kuidas ning kus ta saab vajadusel nõustuda või loobuda isikuandmete kasutamise nõusolekust või esitada vastuväiteid automatiseeritud töötlemisele. Sellisel lahendusele võiks liita ka erasektori organisatsioonid, kes isikuandmeid kasutavad. Nii saaks igaüks “suure pildi” suurest osast oma isikuandmete kasutamisest.
2. Analüüsida igasugust tehisintellekti kasutatavat otsusetegemist inimõiguste seisukohast, lähtudes eesmärgist, et tehisintellekti abil tehtavad otsused peaksid vähendama, mitte kristalliseerima diskrimineerimist.
3. Julgeoleku valdkonnas profileerimist kasutades keelata profileerimine eriliiki tunnuste alusel.
4. Analüüsida plaanitavaid ja juba toimivaid andmekogusid võimalikult väheste isikuandmete kasutamise põhimõtte seisukohast.

TEEMA 2

**ISIKUANDMETE KAITSE ÜLDMÄÄRUSE
(GDPR) RAKENDAMINE**

TEEMA 2: ISIKUANDMETE KAITSE ÜLDMÄÄRUSE (GDPR) RAKENDAMINE

Euroopa Liidu isikuandmete kaitse üldmäärus jõustus 25. mail 2018. See tõi isikuandmete kaitse reeglite jõustamisse uued võimalused ning täpsustas varem kehtinud põhimõtteid. Üldmäärus on otsekohalduv õigusakt, mis tähendab, et Eesti isikuandmete kaitse seadus reguleerib vaid neid osasid isikuandmete kaitsest, mida üldmäärus ei reguleeri või mis üldmääruse kohaselt vajavad siseriiklikult täpsustamist. Üldmäärus EL õigusaktina on Eesti õiguse suhtes ülimuslik.

Üldmääruse tõhus rakendamine Eestis ja mujal riikides on olnud samas problemaatiline.

Esmalt on Eesti järelevalveasutus Andmekaitse Inspeksioon alarahastatud isikuandmete kaitse üldmäärusega talle seatud ülesannete täitmiseks. Sealhulgas ei ole AKIle eraldatud üldse täiendavaid vahendeid võrreldes varasema olukorraga, kuigi üldmäärusega täienes ameti pädevus ja kohustused. AKI võimekus tõhusat järelevalvet teostada on seetõttu kaheldav. GDPR jõustumisele vahetult järgnenud perioodi jäi ka AKI peadirektori venima jäänud vahetumine, mis nõrgestas asutust veelgi.

“Ma arvan, et hästi informeeritud ja teadlikust kodanikust on suur puudus. Kuhu riik ei saa minna, on erasektor, pluss teadusuuringute puhul ei saa ka sekkuda – aga teadusuuringutes on eetika kaheldava väärtusega.”

–fookusgrupis osalenud ekspert

“Riik kuulab akadeemilist eksper-
tiisi, aga nt GDPRiga on teadmatust,
 kuidas tõlgendada, kartes võtta
 otsustust, delegerides selle AKI-
 le, kes pole väga huvitatud, dele-
 gerides selle eetikakomiteele...
 Teadmatust on väga palju erinevate
 asutuste poolt, GDPRi tõlgendamine
 konkreetsetes kontekstides on veel
 sisse seadmata. Andmed on eest ära
 läinud, õigus longib sabas.”

–fookusgrupis osalenud ekspert

Teisalt on üldmääruse jõustumisega olnud vajalik üle vaadata Eesti senine õigusraamistik. Isikuandmete kaitse seaduse rakendamise seadus, millega tehti muudatused teistes Eesti seadustes, et need oleksid kooskõlas üldmäärusega, võeti vastu kiirustades ning põhjalikult muudatusi analüüsimata. Probleemseks võivad osutuda eelkõige üldmääruse artikkel 23 alusel tehtud erandid, millega on liikmesriikidel lubatud piirata üldmääruses toodud kohustusi ja õigusi teatud konkreetsetel eesmärkidel (avaliku huvi, julgeoleku jne põhjustel). Samas peavad need meetmed austama põhiõiguste ja -vabaduste olemust ning olema demokraatlikus ühiskonnas vajalikud ja proportsionaalsed.

Lõpuks on teadlikkus isikuandmete kaitse üldmäärusest üldiselt madal, sest riik ei ole täitnud oma kohustusi inimesi ja ettevõtteid uutest reeglitest teavitada. Samuti ei ole Eestis täna ühtegi vabaihendust, mis otseselt GDPR jõustamisega tegeleks ning aitaks inimestel oma õiguste eest seista. Sellise võimaluse üldmääruse artikkel 80 vabaihendustele annab.

Samuti on eriti suure riskiga isikuandmete töötlemine teaduslikel eesmärkidel, mille puhul ei ole täna selgust, kuivõrd see on üldmäärusega kooskõlas. Kuigi üldmäärus lubab 11 Ma arvan, et hästi informeeritud ja teadlikust kodanikust on suur puudus. Kuhu riik ei saa minna, on erasektor, pluss teadusuuringute puhul ei saa ka sekkuda – aga teadusuuringutes on eetika ka-
heldava väärtusega. –fookusgrupis osalenud ekspert erandina

statistilistel, ajaloolistel ja teaduslikel eesmärkidel isikuandmeid töödelda, on suur risk, et algselt teadustöökäsitatavad isikuandmeid (näiteks mobiiloperaatorite asukohtaandmed, geeni- ja terviseandmed) kommertsialiseeritakse teadusasutuste sidusettevõtete poolt viisil, mis rikub inimõigusi. Taolised rikkumised on varjatud, aga potentsiaalselt eriti kõrge riskiga, kuna puudutavad inimese kõige eraelulisemaid andmeid. Lisaks avalikele andmebaasidele võidakse andmebaasid siduda ka eraandmetega.

VÕIMALUSED JA OHUD

Üldmäärus kujutab endast suurt sammu edasi selle suunas, et isikuandmete kaitse kõrge tase oleks tagatud. See on võimalus nii riigile kui ettevõtetele viia oma tegevus inimõigustega kooskõlla ning tagada eraelu puutumatust austavad infotehnoloogilised lahendused. Isikuandmete kaitse põhimõtete austamine panustab omakorda sellesse, et suureneb usaldus infotehnoloogilistesse lahendustesse ja seega saavad need paremini levida ja leiavad suuremat vabatahtlikku kasutust. Seega kaitseb üldmääruse tõhus rakendamine **õigust isikuandmete kaitsele** ning sellega seonduvat **eraelu puutumatust**.

Tugeval isikuandmete kaitse rakendamisel on positiivne mõju ka teistele inimõigustele, nagu **õigusele väljendusvabadusele** (hoiatakse ära jälitusega kaasnev nn chilling effect).

Isikuandmete kaitse üldmääruse tõhus rakendamine võib samas vajada tasakaalustamist teiste inimõigustega ning piirata mõnevõrra näiteks **ettevõtlusvabadust** või **meediavabadust**.

LAHENDUSED JA SOOVITUSED

1. Vaadata üle Eesti õigusruum isikuandmete kaitse üldmäärusega kooskõla mõttes ning lähtuda lõimitud ja vaikumisi isikuandmete kaitse põhimõttest.
2. Teavitada laialt ja lihtsasti arusaadavalt isikuandmete kaitse reeglitest ettevõtjaid, avaliku sektori töötajaid ja kodanikke, sh konverentside, koolitusprogrammide, kampaaniate ja muu abil.
3. Reguleerida selgemalt ja täpsemalt isikuandmete kasutamine teaduslikel eesmärkidel (näiteks käitumisjuhustega) ning tugevdada järelevalvet piisavate kaitsemeetmete kasutamise üle.
4. Luua vabaühendustele rahastusmeede, mille abil nad saaksid isikuandmete kaitse üldmääruse jõustumisele kaasa aidata, sealhulgas esindades andmesubjekte kohtuvaidlustes artikkel 80 alusel.

TEEMA 3

**VÄLJENDUSVABADUS
INTERNETIS**

TEEMA 3: VÄLJENDUSVABADUS INTERNETIS

Digitaalõiguste valdkonnas on üheks suuremaks väljakutseks väljendusvabaduse tagamine sotsiaalmeedias viisil, mis ei soodustaks samas vaeuudiste levikut, terrorismi, laste kuritarvitamist või vaenu õhutamist.

Ühest küljest on sotsiaalmeedia platvormid toonud erakordsed võimalused omavahel suhelda ning olla püsivas kontaktis inimesetega, kes võivad elada tuhandete kilomeetrite kaugusel. Need on aidanud inimestel organiseeruda, samuti on sotsiaalmeedia platvormid pannud aluse ning aidanud kaasa ettevõtluse arengule. Ligipääs infole ja kättesaadava info laius on võtnud hoomamatult suured mõõtmed.

Sotsiaalmeedia platvormid ise ei ole aga piisavalt pingutanud, et oma platvormidel reeglite järgmist tagada. Facebooki süüdistatakse selles, et aitas Myanmaris kaasa Rohingyade genotsiidile. Facebook, Twitter ja YouTube annavad valimatult platvormi neile, kelle eesmärgid on inimõiguste mõtte vastased.

Omaette probleem on inimõiguste üle otsuste tegemise andmine suurkorporatsioonidele nagu Facebook ja Google, kelle jaoks lõpuks on kõige olulisem siiski nende enda maine ja äri, mitte inimeste põhiõigused. Vaid käputäis suuri korporatsioone, mis asuvad peamiselt USAs, kontrollivad täna platvorme, kus enamik

inimestest oma väljendusvabadust kasutab. Neil on enneolematu võim vaigistada või võimendada.

Praegu toimub sotsiaalmeedias ebasobiva sisu eemaldamine peamiselt kümnete ja kümnete tuhandete töötajate abil, kes kasutajate teavitatud sisu üle vaatavad ja siis vastavalt ettevõtete sise-eeskirjadele sisu kas eemaldavad või mitte. Sotsiaalmeediaplattformide reeglid võivad olla või näida diskrimineerivad või ebaõiglased, sest nad rakendavad oma reegleid sageli ebaselgete kriteeriumite alusel. Ühest küljest peavad nad kontrollima kooskõla enda eeskirjadega, teisalt ka nende reeglitega, mis kehtivad riikides, kus nende platvormi kasutatakse, ning lõpuks muidugi ka universaalsete inimõigusnormidega.

VÕIMALUSED JA OHUD

Sotsiaalmeedia on loonud uued võimalused **väljendusvabaduse** kasutamiseks, samuti ühinemisvabaduseks ja info saamiseks. Sotsiaalmeedia kaudu saab lihtsalt ja kiirelt reageerida inimõiguste rikkumistele.

Sotsiaalmeedia ohustab **õigust elule, vabadusele ja turvalisusele**, kui võimaldab levitada näiteks terroristlikku sisu, laste seksuaalset kuritarvitamist või õhutada genotsiidile või vaenule.

Ohustatakse ka **õigust tervisele ja õiglastele töötingimustele**, sest töötamine sisu modereerijana ei pruugi hästi mõjuda vaimsele tervisele. Samuti võidakse ohustada.

LAHENDUSED JA SOOVITUSED

1. Pöörata senisest enam tähelepanu sotsiaalmeediaplatvormide inimõigustest kinnipidamisele. Kasutada teiste riikide eeskujul võimalusi survestada platvorme inimõigustest ja Eesti Põhiseadustest ning teistest seadustest kinni pidama.
2. Suurendada teadlikkust sotsiaalmeedia kasutamisega seotud ohtudest ja viisidest ennast kaitsta, eelkõige laste ja noorte seas. Lahendused ja ideed teadlikkuse tõstmiseks.

“Kui me tahame parandada olukorda, siis meditsiinimetafooride eeskujul peaks andma lihtsaid soovitusi (mitte koolitada kõiki immunoloogideks, vaid öelda, et pese käsi). Eialgu peaks tulema väga praktilised soovitused, sinna peale tuleb inimõiguste kiht, sinna peale tehniline pool.”

–fookusgrupis osalenud ekspert

IDEED TEADLIKKUSE TÕSTMISEKS:

Ekspertidega kohtumistest võrsus palju häid ideid nii teadlikkuse tõstmiseks kui muul viisil inimõiguste paremaks kaitseks digitaalvaldkonnas.

- lihtsas keeles ja lugusid jutustavad teavituskampaaniad, mis kasutavad visuaalset keelt ning ei oleks keelud ja käsud, vaid pigem positiivsest lood
- artiklid ja lood ebatraditsioonilistes kohtades, nt naisteajakirjades
- haridussüsteemis viia teemad sisse juba alusharidusest
- plaanitav MOOC gümnaasiumiõpilastele
- paroolimuutmise päev
- alternatiivse narratiivi vajalikkus
- levitada avatud lähtekoodiga platvorme, nn “fair trade” tehnoloogiaid
- luua lihtsad tarkvarakomplektid, mida inimesed saavad kasutada
- tunnustada eetilisi ettevõtteid, mis inimõigusi austavad, ning häbimärgistada neid, mis reegleid ei järgi

EESTI INIMÕIGUSTE KESKUS JA DIGITAALÕIGUSED

Eesti Inimõiguste Keskus (EIK) on sõltumatu valitsusväline inimõigusorganisatsioon, mille missioon on luua koos toetajatega iga inimese inimõigusi austav Eesti. Keskuse visioon on olla aastaks 2020 mõjus ja pädev Eesti sõltumatu inimõigusliikumise eestvedaja.

EIK korraldab oma tegevust vastavalt ühiskondlikele vajadustele. Meie fookuses on võrdne kohtlemine ja mitmekesisuse edendamine, varjupaigataotlejate ja pagulaste inimõigused. Oleme Eesti mitmekesisuse kokkuleppe koordinaatorid. Jälgime üldist inimõiguste olukorda Eestis ning avaldame 2007. aastast aruannet inimõiguste olukorrast Eestis. Oleme ÜRO pagulasameti UNHCR partnerid Eestis.

EIK tegevus digitaalõiguste valdkonnas on seni olnud piiratud, aga käesoleva projekti raames uurime võimalusi, kuidas strateegiliselt sekkuda.

2014. aastast oleme aeg-ajalt tegelenud sideandmete säilitamise teemaga. Oleme olukorda uurinud ning küsinud korduvalt infot erinevate asutuste ja ettevõtete käest, et paremat ülevaadet saada.

Oleme ka pöördunud riigi poole ettepanekuga lõpetada ebaseaduslik sideandmete säilitamise kohustus ning reguleerida täpselt ja selgelt sideandmete kasutamine. Osaliselt ka meie töö tulemusel algatas justiitsministeerium 2018. aasta lõpus seaduseelnõu väljatöötamiskavatsuse. Oleme tegelenud koostöös Euroopa Põhivabaduste Ühendusega LIBERTIES internetis leviva käitumusliku reklaami teemaga, mille osas esitasime samaaegselt mitmete teiste sõltumatute inimõigusorganisatsioonidega kaebuse järelevalveasutusele (Eestis Andmekaitse Inspeksioon), et need uuriks käitumusliku reklaami kooskõla isikuandmete kaitse reeglitega.

Vaenukõne piiramiseks internetis teeme koostööd Euroopa Komisjoni ja sotsiaalmeediaplatvormidega, et seirata regulaarselt vaenukõne sisaldava sisu eemaldamist. Lisaks oleme partnerid projektis Op-Code, mille eesmärkideks on laiendada ja tugevdada kodanikuühiskonna organisatsioonide koalitsiooni, mis tegeleks süstemaatiliselt online-vaenukõne monitoorimisega; ning avatud koodi lahenduste arendamine ja edendamine, mis võimaldaksid modereerida vaenulikku sisu.

Oleme tehnoloogiaga seonduvaid teemasid kajastanud järjepidevalt inimõiguste aruannetes, eelkõige eraelu puutumatus käsitlevates peatükkides.

Toeta Eesti Inimõiguste Keskuse
tegevust püsiannetusega kodulehel

www.humanrights.ee/anneta



EESTI INIMÕIGUSTE KESKUS 2019