PRIVAATSUSÕIGUS INIMÕIGUSENA JA IGAPÄEVATEHNOLOOGIAD

Uuringu teoreetilised ja empiirilised lähtealused

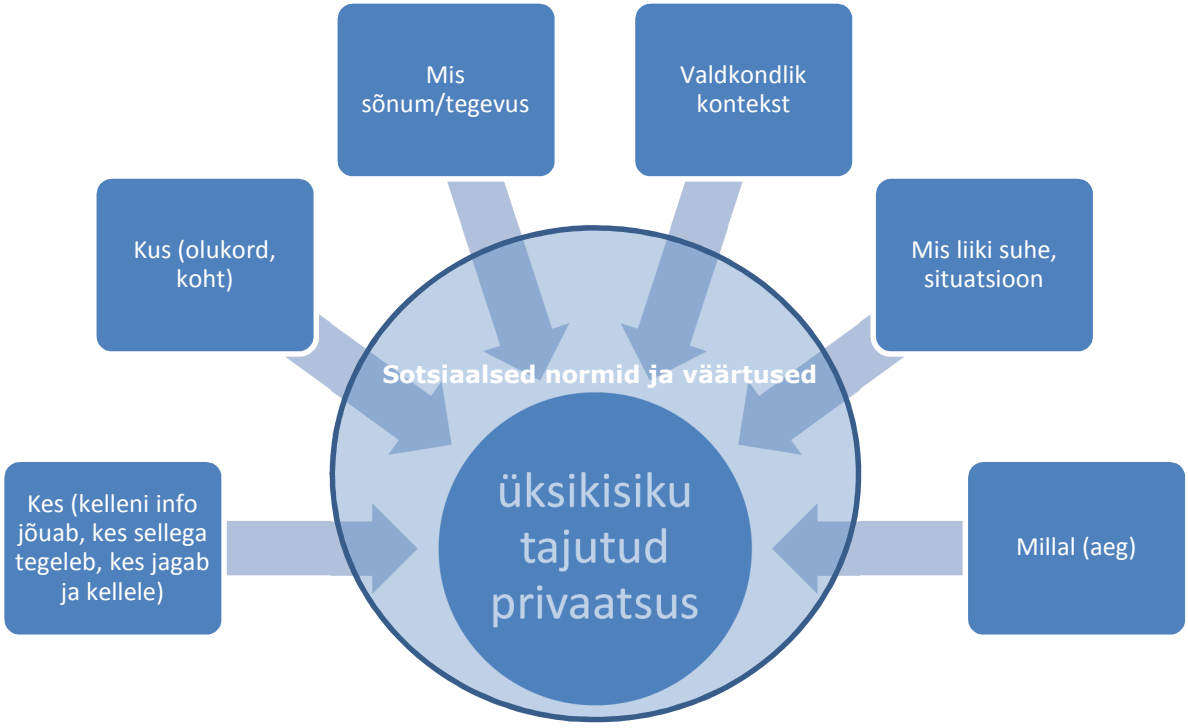
Maria Murumaa-Mengel
Pille Pruulmann-Vengerfeld
Katrin Laas-Mikko

SISUKORD

SISSEJUHATUS

PRIVAATSUS KESKSE TEEMANA. Tänapäeva ühiskonnas on **privaatsusega seotud probleemid sageli tajutavad suurematena kui kunagi varem** inimkonna ajaloos. Ühelt poolt on tegemist näilise privaatsuse kadumisega, sest väikeses kogukonnas või peres koos elades oli saladust ehk raskemgi pidada. Teisalt on aga digitaaltehnoloogia ning uus meedia muutnud informatsiooni jagamise, vastuvõtu ning salvestamise praktikaid, esitades meie privaatsuse kaitsmisele suure väljakutse. Käesolev uuringu osa keskendub ennekõike **informatsioonilisele privaatsusele** ehk **informatsioonilisele enesemääramisele**. Andmete kiire otsitavus, silmapilkne edastus, püsivus ning lõputu kopeerimisvõimalus on vaid mõned digitaaltehnoloogiaga kaasnevad nähtused, mis ohustavad privaatsust ning muudavad avaliku ja privaatse või ühiskondliku ja erasfääri vahele piiri tõmbamise keeruliseks. Kuigi avaliku arutelu objektiks on eelkõige olukorrad, kus privaatsust rikuvad teised osapooled (näiteks Euroopat raputanud luureskandaalid või WikiLeaks, samuti suurettevõtete, nagu Google, Facebook ja Amazon, kontroll üksikisiku andmete ja käitumise üle), siis samavõrd on privaatsust riivavate olukordade taga ka üksikisikud ise, jagades endale aru andmata erinäolist materjali ning andes ise nõusoleku oma andmete kasutamiseks eri olukordades. Nii ongi privaatsuse kui põhiõiguse kaitse tingimustega seoses mõistlik küsida, **mil määral me peame kaitsma inimest tema enda eest?**

KONTEKSTI TÄHTSUS. Privaatsusõiguse uuringut alustades olime keeruka küsimuse ees, mida üldse peaks uurima, sest kõikvõimalikke privaatsust rikkuvaid või riivavaid olukordi on lõpmata palju. Need moodustuvad sageli kaleidoskoopilise mustri kontekstist, osapooltest, sõnumist ja ajast, mida tajutakse läbi sotsiaalsete normide ja väärtuste prisma (vt joonis 1). Need tegurid on omavahel tihedalt seotud ja pidevas muutumises. Nii võib info selle kohta, et oleme parasjagu kodust ära, olla vajalik naabrile selleks, et naabrivalvet teostada, kuid privaatsust riivav võõra tõttu, kes võiks meie kodu sel ajal ohustada. Või näiteks oleme väga rõõmsad, kui arst jagab meie terviseinfot teise arstiga ning selle tulemusel jõutakse parematele raviotsustele, kuid meie privaatsus oleks sügavalt riivatud, kui terviseinfost teadlikuks saades võiks tööandja otsustada meie ametialase suhte üle. Ka on Eestis ning mujal sageli küsitud tööandja õiguse piiride kohta – kas töömeil on privaatne või avalik? Kas tööintervjuul peale CV ka kandidaadi sotsiaalmeediakontot uurida on sobilik? Kui parafraseerida Pille Runnelit, kes ütles, et igal inimesel on „oma internet, mis on seotud tema enese oskuste, harjumuste ja vajadustega" (Runnel 2010), siis saame öelda, et **igal inimesel on ka oma unikaalne situatsioonist sõltuv privaatsus.** Kuna inimene ei ela aga sotsiaalses vaakumis ning ühiskonnast eraldatuna, tuleb arvestada, et inimese „oma" privaatsust on mitmeti mõjutanud kontekst – mida tajutakse privaatsena, mis on kontekstiga (sotsiaalsed normid, ajaline ja ajalooline eripära jne) läbi põimunud.



Joonis 1. Kontekstilist privaatsust mõjutavad tegurid

Mõned autorid on selgel seisukohal, et privaatsust tänapäeva infoühiskonnas saab selgitada üsna lihtsalt: see puudub! Käesolevas uuringu osas on siiski eeldatud, et privaatsuse kaitseks on võimalik rakendada erinevaid strateegiaid. Informatsioonilise privaatsuse puhul saab eristada **objektiivset privaatsuse rikkumist** ja **tajutud ohtu privaatsusele** – need võivad, ent ei pruugi olla alati omavahel seotud ning käesolevas uuringus keskendutakse tajutud ohule. Näiteks on juriidiliselt kõik korras, kui inimene on nõustunud mingi teenuse kasutamistingimustega, seda loetakse informeeritud nõusolekuks. Inimene võib aga teatud lepingupunktide rakendumisel tunda oma privaatsuse riivet, ehkki õiguslikult ei ole privaatsust rikutud. Käesoleva uuringu eesmärk ei ole teha kindlaks, kas mingi olukord on privaatsuse rikkumine eetilises või õiguslikus mõttes, vaid vaadelda, kuidas inimesed eri olukordi tajuvad ja millised olukorrad nende arvates potentsiaalselt privaatsust rikuvad.

Käesoleva uuringu osa eesmärk on anda põgus ülevaade privaatsusega seotud teoreetiliste põhimõistete ja -probleemide ning erinevate läbiviidud uuringute ja küsitluste kohta, samuti selgitada uuringu teoreetilisi ning empiirilisi lähtealuseid.

Alljärgnevalt:

- esitatakse ülevaade privaatsuse laiema käsitluse kohta ja ka kitsamalt internetiprivaatsuse kohta;
- võetakse kokku põhilised võimalikud tajutavad privaatsuse riived;
- tuuakse välja probleeme üksikisiku suhetes riigi, tööandja, teenusepakkuja ning teiste inimestega;

- tutvustatakse, millised on eestlaste vaated privaatsusega seonduvale võrdluses Euroopaga.

PRIVAATSUSE MÕISTE

PRIVAATSUSE KOMPONENDID, ERINEVAD PERSPEKTIIVID. Privaatsuse kontseptsioon võib hõlmata endas laialdast huvide, õiguste või aspektide valikut. Näiteks toob David Solove (2002) välja **kuus privaatsuse eri aspekti**: õigus olla rahule jäetud; piiratud ligipääs endale (füüsilisele isikule), võimalus end kaitsta soovimatu juurdepääsu eest; teatud asjade teiste eest varjamise õigus; kontroll isikliku informatsiooni üle; oma väärikuse, individuaalsuse ja isiku kaitse ning õigus intiimsusele – inimesel on õigus kontrollida ja piirata juurdepääsu informatsioonile, mis puudutab tema lähisuhteid või eluaspekte.

Mitmed privaatsust käsitlenud autorid (Allen 1997, DeCew 1997, Rössler 2005) on eristanud **kolm privaatsuse valdkonda või sfääri**: informatsiooniline privaatsus (*informational privacy*), füüsiline või ruumiline privaatsus (*physical, local, spatial privacy*) ja otsustusprivaatsus (*desicional privacy*). Käesolevas uuringu osas keskendutakse eelkõige informatsioonilisele privaatsusele, mis hõlmab inimese kohta kogutud, salvestatud ja jagatud andmeid.

Erinevad filosoofid ja õpetlased (näiteks Gross 1967, Miller 1971, Bennett 1992, Post 2001) on väitnud, et ei ole võimalik välja tuua selget ja konsensuslikku kokkulepet selle kohta, mida privaatsus tähendab. **Privaatsuse mõiste on väga kompleksne ja vastuoluline**. Arutelu muudab keerukaks see, et privaatsuse mõiste määratlemisel räägitakse samal ajal ka privaatsuse väärtusest ehk sellest, missugune roll on privaatsusel üksikisiku ja ühiskonna jaoks, ning sellest tulenevalt ka privaatsuse piiridest ja kaalutlemisest teiste väärtuste suhtes.

Suur osa privaatsuse teoreetikuid (Westin 1967, Rachels 1975, Fried 1984, Rössler 2005 jt) peavad privaatsuse puhul keskseks **kontrolli enesekohase informatsiooni üle**. Üks tuntumaid privaatsuse teoreetikuid Alan Westin (1967: 7) on määratlenud privaatsuse üksikisikute, gruppide või institutsioonide õigusena määrata kindlaks, millal, kuidas ja millises ulatuses nende kohta käivat informatsiooni teistele edastatakse. See tähendab seda, et privaatsuse määr või see, kas andmesubjekti privaatsust on rikutud või mitte, sõltub tema enda valikust: kuivõrd ja millist teavet ta soovib kaitsta. Selle aluseks on liberalistlik isiku enesemääramise idee – isik on iseend määratlev ja vaba otsustama, millised väärtused on tema jaoks olulised.

Kontrolli idee näib olevat kõikehõlmav ning absoluutne, mistõttu tänapäevased privaatsuse mõiste määratlused kitsendavad veidi varasema mõiste ulatust ja rõhutavad pigem **isiku õigust otsustada, kes ja mil määral saab juurdepääsu teda puudutavale informatsioonile ja ka kasutada seda** (Rössler 2005, Moore 2008 jt). Privaatsusõigus sisaldab sel juhul juurdepääsu kontrolli, kuid ka kontrolli informatsiooni kasutamise õiguste üle. Nimetatud õiguse keskmes on isiku (informeeritud) nõusolek koguda / juurdepääs saada

tema isikuandmetele mingil konkreetsel eesmärgil, näiteks selleks, et sooritada oste mõnes e-poes. See nõusolek ei anna automaatselt nõusolekut andmete kasutamiseks mõnes muus kontekstis või situatsioonis mingil muul eesmärgil.

PRIVAATSUS INTERNETIS

ISIKLIK VASTUTUS OMA PRIVAATSUSE KAITSMISEL. Niisiis on inimesel õigus kontrollida juurdepääsu teda puudutavale informatsioonile ja selle kasutust. Helen Nissenbaum (1998) on aga rõhutanud, et see õigus ei pruugi kehtida siis, kui inimene ise on informatsiooni avalikustanud ning ei ole teinud olulisi pingutusi, et seda avalikust ruumist eemaldada. Sotsiaalmeediakeskkondade ajastul on just see aspekt üks problemaatilisemaid, kuna internetti sattuvast infost märkimisväärne hulk on inimeste enda üles laetud, Terence Craigi ja Mary Ludloffi (2011) järgi on koguni 70% digitaalsest maailmast loodud inimeste poolt Facebooki, Twitteri, LinkedIni, Flickri, YouTube'i ja teiste sarnaste teenuste kasutamisel.

IKT LEVIKU MÕJU PRIVAATSUSELE. Info- ja kommunikatsioonitehnoloogia (IKT) kiire arengu ja üldiselt kättesaadavaks muutumise oludes on tehnoloogia – eelkõige internet, arvutid ja mobiiltelefonid – kodustatud (*domestication*), omaks võetud ja integreeritud igapäevaellu. Lääne kultuuris isegi sel määral, et räägitakse IKT-rikkast magamistoakultuurist (Bovill ja Livingstone 2001). Igapäevatehnoloogiate puhul on oluline märgata nende **kasutusvõimaluste suurt potentsiaali** (pangandusest pornoni), **pidevat kasutusvalmidust** (mobiilsus, kiire ühendus), **suurt kasutajate hulka** (kriitiline mass) ning **sotsiaalseid rituaale ja rutiine**, millega need tehnoloogiad on seotud (näiteks kohtingukaaslase guugeldamine, pühapäeviti vanaemaga skaipimine, avalikus kohas kõrvaklappidega isikliku audioruumi loomine jne). Tehnoloogia on saanud meie füüsilise mina laienduseks ning oma pideva kohalolu tõttu muutunud nähtamatuks, muutes seeläbi mõnikord nähtamatuks ka võimalikud privaatsust riivavad olukorrad. Kui Michel Foucault' (1991) kõneles ühiskonna puhul panoptikonist (vähesed jälgivad-valvavad paljusid) ja Thomas Mathiesen (1997) televisioonist kui sünoptikonist (paljud vaatavad väheseid), siis Jakob Linaa Jensen (2010) ja Jeffrey Rosen (2004) on rääkinud omnoptikonist – pidev üksteise jälgimine, nii-öelda ühisvalve, mis iseloomustab uue meedia keskkonda. Sotsiaalvõrgustikes toimuvat on nimetatud ka osalusjälgimiseks (Albrechtslund 2008): paljud vaatavad paljusid, tehes seda omavaheliste suhete- ja sõprusvõrgustike ning linkide kaudu. Keegi kasutajatest ei tea kunagi, kes neid parasjagu jälgib. **Avaliku ja privaatse elu piire on oluliselt ähmastanud sotsiaalvõrgustike vahendatud avalikkus**. Kui seda võrrelda klassikalise arusaamaga avalikust ruumist (pargid, tänav, kohvikud jne), kerkib esile neli põhilist eristavat unikaalset tunnust (boyd 2007).

1. Püsivus. 15aastasena tehtud teod ja väljaöeldud arvamused on kättesaadavad ja nähtavad inimese vanemaks saades, arvestamata seda, et inimese hoiakud ja hinnangud on muutunud.
2. Otsitavus. Avaldatud infot on võimalik vähese vaevaga internetiavarustest üles leida.
3. Kopeeritavus. Digitaalne info on kergesti kopeeritav ning seega on võimalik infot ühest kontekstist teise tõsta, samuti algset infot märkamatult moonutada.
4. Nähtamatu auditoorium. Vahendatud avalikkuses ei näe me enda jälgijaid ning eelmised kolm tunnust muudavad piilujatele kättesaadavaks aja ja ruumi, milles nad ise osalised olnud ei ole.

Probleem on selles, et inimese elu võib jagada erinevatesse sotsiaalsetesse situatsioonidesse, millel kõigil on oma auditoorium ja kontekst (boyd 2008). Ametialastes suhetes jagatakse üht tüüpi infot, lähedaste sõpradega suheldakse teist moodi ja oma lastega kolmandal moel. Või näiteks raviasutuses annab patsient infot enda meditsiinilise tausta kohta, samas aga ei tohi seda informatsiooni küsida näiteks tööintervjuul (Baghai 2012). **Uus meedia on seganud kokku erinevad kontekstid, mis muidu olid eraldiseisvad, auditoorium on nähtamatu ja materjal püsiv**.

INTERNETIPRIVAATSUSE KAITSMISE STRATEEGIAD. Ometi viitab danah boyd [sic!] (2008) sellele, et meie praegune olukord ei ole nii ainulaadne kui meile meeldib rõhutada – ajaloost saab tuua palju näiteid, kus ülikontrollivast eraellu tungivast režiimist hoolimata on inimesed välja arendanud strateegiaid, kuidas teatud osas siiski privaatsus säilitada. Internetiprivaatsuse kaitsmiseks kasutatavaid strateegiaid on mitu. Tagasihoidlik teabe kasutamine, enesetsensuur ja kontode ning info kustutamine (Oolo ja Siibak 2013) on neist strateegiatest lihtsaimad, kuid nende tegelikus tõhususes võib kahelda, sest inimene alahindab pidevalt oma auditooriumi suurust ning info võib olla kustutamise hetkeks juba mitu korda muudele saitidele kopeeritud. Veebikeskkonnad võimaldavad kasutajatel rakendada ka erinevaid privaatsussätteid, mille kaudu saab kontrollida saadetava sõnumi otsese auditooriumi suurust. Samas on seadete muutmine aega ja pingutust nõudev ning osale veebikasutajatele ka üle jõu käiv. Veel võiks tähelepanu juhtida sellele, et vaikimisi seaded on tihti sellised, mis jätavad võimalikult palju kasutaja informatsioonist avalikuks – privaatsus on miski, mille nimel peab eraldi pingutama, see ei ole vaikimisi seade. Euroopa Liit pöörab praegu andmekaitseseaduse reformi käigus muu hulgas just sellele aspektile tähelepanu: **andmekaitse meetmed ja seaded peaksid olema teenustesse ja toodetesse algselt sisse disainitud ning vastupidiselt praegu levinud olukorrale peaks eraldi tähelepanu ja tegevust nõudma andmete avaldamine, mitte kaitsmine** (Progress on EU... 2014).

NÄITEID PRIVAATSUSE KAITSE KOHTA. Inimestel on võimalik kasutada privaatsuse kaitse strateegiana veebis mitut identiteeti, esitada valikuliselt valeinfot või tegutseda sootuks anonüümselt (Oolo ja Siibak 2013). Peale selle on üks privaatsuse osalise säilitamise võimalus sotsiaalne steganograafia – teadlik mitmetähenduslike sõnumite saatmine, mis võimaldab osal auditooriumist mõista sõnumit ühtmoodi ja teisel osal teistmoodi (boyd ja Marwick 2011, Siibak ja Murumaa 2011). Steganograafia on ajaloost tuntud meetod, mida kasutati selleks, et peita sõnumeid kõigi pilkude all – nähtamatu tint, piimaga kirjutamine, piltmõistatused ja salakeeled (boyd 2010). Sotsiaalvõrgustikes kasutatakse sarnast meetodit, postitades näiteks lause, mille sisu on osale auditooriumist mittemidagiütlev, kuid teatud kitsale sihtrühmale, kes on kontekstiga paremini kursis ja kes omavad sõnumi dekodeerimiseks vajalikku tõlgenduslikku perspektiivi, on see aga sügava tähendusega sõnum, mis informeerib neid näiteks sõnumi saatja hingelisest seisundist, viimastest toimunud arengutest või hoiakutest (boyd 2010). Ühes Eurobaromeetri uuringus uuriti inimeste suhtumist privaatsusesse ja sellega seotud tavasid (Eurobaromeetri eriuuring 359, 2011) ning selgitati välja, et eurooplased kasutavad enim tagasihoidlikku teabe jagamist ning tehnilisi ja protseduurilisi strateegiaid, näiteks teabele juurdepääsu piiramine, rakendades veebikeskkonna pakutavaid tööriistu ning kasutades turvalise ühendusega lehekülgi ja turvatarkvara.

Mõned radikaalsemad autorid, näiteks Simson Garfinkel (2001) ja David Brin (1998), on koguni väitnud, et privaatsus on surnud ja me peaksime harjuma mõttega, et ühiskond ongi ülimalt läbipaistev. Brin (1998) hoiatas ühtlasi, et suurim oht on jälgimistehnoloogiate kättesaadavus, mis on tänapäeval saanud suurel määral tegelikkuse osaks – **kui kõik inimesed omavad juurdepääsu samale informatsioonile, on võimusuhted võrdsed ning toimub lausjälgimine**. Ka Facebooki looja Mark Zuckerberg on väitnud (Kirkpatrick 2010), et privaatsuse ajastu on möödas ning et vaid inimesed, kellel on midagi varjata, muretsevad privaatsuse pärast. Samasugust argumenti on eelnevalt kasutanud feministlikud teoreetikud ja kommunitaristid, kes rõhutavad, et privaatsus individualistliku väärtusena toetab anonüümsust ning selle varjus sotsiaalselt taunitavat käitumist ja priileivasöömist teiste kulul. Selle väite sisemisele loogikaveale on tähelepanu juhtinud Solove (2007), kes rõhutab selle väärarusaamal põhinemist – et privaatsus seisneb halbade tegude ja valesti käitumise varjamises. Igal inimesel on kellegi eest midagi varjata. Näib, et **privaatsusest kõnelemisel on takerdutud eelkõige teabe varjamise ja piiramise konteksti**, nagu see oli privaatsuse temaatika esmakäsitlejate puhul (Warren ja Brandeis 1890, Cooley 1880). Lisaks peavad mul-pole-midagi-varjata-argumendi kasutajad sageli silmas seda, et neil ei ole midagi varjata selle kujutletava auditooriumi eest, kellele postitades mõeldakse, kuid mitte kõigi nende eest, kes postitust internetis näha võivad (Siibak ja Murumaa 2011).

PRIVAATSUSE VÄÄRTUS JA SELLE RIIVAMINE

PRIVAATSUSE VÄHENEMISE POSITIIVSED ASPEKTID. Loomulikult on läbipaistvam, alati kõike mäletav infoühiskond loonud inimestele palju uusi võimalusi, mille puhul saame näha privaatsuse vähenemist positiivsena: enda kohta info jagamisel on oluline roll sõprussuhete säilitamisel ning virtuaalvõrgustikus enda kohta käiva info avaldamine on osaliselt ka usalduse demonstreerimine kaaslastele (Marwick, Murgia-Diaz ja Palfrey 2010). Malene Charlotte Larsen (2007) on toonud isikliku info avaldamise puhul välja teiste hulgas näiteks järgmised positiivsed aspektid, miks internetis ennast eksponeeritakse ja milline on selle mõju: internetis toimub pidev enda ja teiste identiteedi (re)konstrueerimine, kogukonnatundele kinnituse saamine ning demokraatia põhimõtete rakendamine oma arvamuse avaldamise ja hääle kuuldavaks tegemise kaudu.

PRIVAATSUS KUI KAITSMIST VAJAV VÄÄRTUS. Avalikkuses ja teadusringkondades toimuvates diskussioonides privaatsuse üle kasutatakse valdavalt ohu diskursust – privaatsus kui pidevalt turmtule all olev, kuid ilmtingimata kaitsmist vajav väärtus. Kuid kõigepealt võiksimegi enda käest küsida, mida privaatsus kaitseb? Miks privaatsust üleüldse väärtustatakse ja miks soovitakse kontrollida juurdepääsu ennast puudutavale teabele või selle kasutamist? Privaatsuse mõistega ei määratleta tegelikult, mis see täpselt on, mida informatsioonile juurdepääsu ja selle kasutamise kontrolliga soovitakse kaitsta.

PRIVAATSUSE KUI VAHENDVÄÄRTUSE FUNKTSIOON. Privaatsust peetakse üldiselt vahendväärtuseks, mida hinnatakse seetõttu, et see kaitseb teisi, võib-olla olulisemaid väärtusi. Ka selles küsimuses ei ole jõutud üksmeelele, kuid üsna paljud autorid väidavad, et

privaatsuse peamine funktsioon on kaitsta isiku autonoomiat ja mina-pildi arengut (Gavison 1980, Schoeman 1984, Kupfer 1987, Rössler 2005, Steeves 2009 jt). Privaatsus annab meile **otsustusõiguse** selle konteksti üle, milles me käitume või tegutseme, et kaitsta seda teiste sekkumise eest ja võimaldada meil kujundada oma elu ning kuvandit endast. **Austus teise isiku moraalse autonoomia vastu** eeldab, et asetame end teise isiku kingadesse ja püüame mõista tema isiklikke eesmärke, hinnanguid, hoiakuid, mõtteid ja soove tema enda seisukohalt (Williams 1973). **Informatsiooniline privaatsus** tähendab isiku õigust otsustada infokeskkonnas, kes ja mil määral saavad juurdepääsu tema teabele ja kasutada seda. Valeria Steevesi (2009) arvamuse kohaselt võimaldab privaatsus lisaks luua **tähenduslikke suhteid teistega**. Steevesi sõnul on privaatsuse otsimine sotsiaalne praktika, mis võimaldab sotsiaalsetel toimijatel tõmmata piiri enda ja teiste vahele, olles suletud või avatud sotsiaalseks suhtlemiseks. Selle teooria kohaselt on sotsiaalsed toimijad võimelised valima, mis on nende jaoks olulisim, ja määratlema end suhetes.

PRIVAATSUSÕIGUSE RIKKUMINE. Privaatsusõiguse rikkumisega võib kaasneda mitmeid ebasoovitavaid tagajärgi isiku jaoks, näiteks identiteedi vargus ja seeläbi juurdepääs isiku varadele või talle määratud hüvedele, ebaõiglus, mida tekitatakse teatud info ärakasutamise või ebavõrdse kohtlemise kaudu, samuti eneseväärikuse riivamine. Riske ühiskonnale on väga keeruline hinnata, kuna reeglina on tegu n-ö **pehme mõjuga**. Me ei tea täpselt, kui paljude inimeste privaatsus ja millises kontekstis peaks olema riivatud selleks, et nad kaotaksid näiteks usalduse oma valitsusasutuste vastu, või selleks, et demokraatia oleks ohustatud.

Privaatsuse kaitsjad räägivad tihtipeale privaatsusest kui õigusest, mis jätab mulje, et tegu on absoluutse õiguse või väärtusega, mida ei tohiks mitte mingil juhul loovutada, ja et privaatsuse konflikt selliste konkureerivate väärtustega nagu solidaarsus, turvalisus või sõnavabadus on vältimatu ja leppimatu. Hiljutised käsitlused eeldavad siiski, et väärtuskonfliktid ja valikud eri väärtuste üle on meie elu loomulik osa pluralistlikus ühiskonnas ja et privaatsust peab saama kaaluda teiste meile oluliste ja mõnikord võrreldamatute väärtustega. Samuti riskime oma privaatsuse riivamisega iga päev, kui avaldame enda kohta tundlikku informatsiooni olulistes suhetes või suhtluskeskkondades ja mujal, sest üldjuhul me ei soovi ju nn ideaalset privaatsust – täielikku eraldatust või anonüümsust ja sotsiaalsetest suhetest kõrvalejäämist. Seega, nagu eelnevalt öeldud, on oluline kontekst.

PRIVAATSUS OHUSTATUD VÄÄRTUSENA. Ka meie uuring lähtub ennekõike küsimusest, kuivõrd tajutakse privaatsust ohustatud väärtusena ja millises kontekstis seda väärtustatakse. Sellise probleemipüstitusega jätame teatud mõttes kõrvale võimaluse, et inimesed on rõõmsad informatsioonilisest privaatsusest loobumise üle. Me ei saa välistada, et see mõningatel juhtudel täpselt nii ei ole, kuid teoreetilised ning empiirilised lähtealused ja ka käesoleva uuringu tulemused näitavad, et privaatsust käsitletakse pigem kui midagi, mis vajab kaitset.

Praeguseni kehtiv Euroopa Liidu andmekaitsedirektiiv (direktiiv 95/46/EÜ) reguleerib teatud kindlaid andmekasutuse valdkondi, mille alusel saab välja tuua **kuus peamist privaatsuse riivamise viisi**.

1. Puudulik teavitamine – inimest, kelle kohta andmeid kogutakse, ei ole sellest teavitatud.
2. Kasutuseesmärgile mittevastamine – kogutud andmeid kasutatakse lubatust erinevatel eesmärkidel.
3. Nõusoleku puudumine – isikuandmeid avaldatakse või jagatakse kolmandatele osapooltele ilma isiku nõusolekuta.
4. Turvaaugud ja infolekked – kogutud andmeid ei käsitleta piisavalt turvaliselt (andmete kuritarvitamine, väärkasutus, vargused, teabe kadumine).
5. Piiratud juurdepääs enda andmetele – inimesel puudub enda kohta kogutud andmetele juurdepääs ning võimalus ebatäpsusi või väärinfot parandada ja ümber lükata.
6. Andmetöötlejate vastutuse puudumine – andmetöötlejad ei vastuta nimetatud põhimõtete täitmise eest.

Euroopa Liit otsib praegu uusi lahendusi, et uuendada nimetatud 1995. aastast kehtivat andmekaitsedirektiivi. Üks põhiline arutelupunkt on internetiprivaatsusega seonduvate õiguste kaitse. Ehkki internetile on globaalsuse tõttu omane universaalsete reeglite puudumine, loodab EL juba käesoleva aasta lõpuks välja töötada kõigi liikmesriikide jaoks sobivad eeskirjad (isikuandmete kaitse üldmäärus). Üks põhimõistetest, mis muudatustega seonduvat diskussiooni juhib, on **õigus andmete kustutamisele** (Euroopa Parlament 2014) – et inimestel oleks õigus nõuda nende kohta käiva info kustutamist internetist. 2014. aasta kevadel tegi Euroopa Kohus otsuse, mille alusel saavad inimesed edaspidi nõuda otsingumootorilt (näiteks Google'ilt) neid käsitlevate ebaõigete isikuandmete kustutamist, muutes sellega otsingumootorid ametlikult andmete töötlejaks (Rebane 2014). Kohus võttis ka seisukoha, et otsingumootor peaks üldreeglina alati eelistama isiku õigust privaatsusele avalikkuse õiguse ees infot saada (Streitfeld 2014). Kriitikud on nimetanud otsust sõnavabaduse piiramiseks ja privaatsuse tsensuuri ajastu algatajaks (Mayes 2011, Index on Censorship 2014).

PRIVAATSUS ERI LAADI SUHETES. Järgnevates alapeatükkides käsitletakse inimeste privaatsusega seonduvaid eri laadi suhteid erinevates eluvaldkondades, inimeste suhteid riigiga, tööalaseid suhteid ettevõtete ja teiste töötajatega. Sellistes aruteludes jäetakse mõnevõrra tagaplaanile fakt, et sageli toimub privaatsuse riive juriidiliselt täiesti korrektsel moel. Tajutud privaatsuse rikkumise põhjus on see, et inimene ise on selle info avalikustanud. Siinkohal tulebki rõhutada seda, et **inimene ise on tihti oma privaatsusele suurim risk**, avaldades eri keskkondades väga erinäolist informatsiooni, mida võidakse kasutada muul eesmärgil kui info avaldaja on endale ette kujutanud. Näiteks pakub sotsiaalmeedias avaldatu huvi nii ettevõtetele (sellest pisut hiljem) kui ka näiteks korrakaitse- ja julgeolekuvallas tegutsevatele organisatsioonidele (Wigan ja Clarke 2013). Politsei kasutab Twitterit ja Facebooki, et jälgida uurimisaluste käike ja tegevusi (Knibbs 2013), Facebooki konto andmete abil saab hinnata inimese laenuvõimet (Nergi 2013, Parksepp 2014) ning kõne all on olnud võimalus, et kohtul oleks õigus inimesega ühendust võtta ka Facebookis (Teder 2012).

Riigi ja inimese vahelised suhted on laialdaselt levinud e-teenuste ja info digitaalse liikumise tõttu nii mitmekülgsed, et kuus eespool nimetatud riivet on neis suhetes potentsiaalselt olemas. Taas tuleb eristada järgnevate arutluste kontekstis objektiivset ja tajutud ohtu – tehniliselt võivad olla andmed kaitstud, aga inimesed võivad siiski tajuda privaatsuse riivamist. Käesolev uuring, samuti näiteks privaatsust käsitlev Eurobaromeetri 2011. aasta eriuuring 359, peab silmas eelkõige privaatsuse tajuga seonduvaid ilminguid, mitte mõõdetavaid konkreetsemaid objektiivseid privaatsuse riiveid.

EESTI NÄIDE. Eesti on maailmas positiivset tähelepanu pälvinud oma mitmekülgsete ning laialt levinud riiklike e-lahendustega (elektrooniline tulude deklareerimine, e-hääletamine, paberivaba valitsus, e-tervis, e-äriregister, e-kool, EHIS jne). Eesti internetikasutajad leiavad, et e-teenustel on olnud neile selgelt positiivne mõju, hoides kokku aega ja muutes asjaajamise lihtsamaks (Kalvet, Tiits ja Hinsberg 2013). Need kaks tegurit, kasulikkus (fookuses eesmärk) ja kasutuskeerukus (fookuses protsess) on kesksel kohal ka tehnoloogia aktsepteerimise mudelis (Davis 1989). Ehkki andmeid kogutakse, töödeldakse ja salvestatakse tänapäeval mitmetes eri andmebaasides, on see paljude jaoks tähelepandamatu või ebaoluline. Näiteks vaid 40% eestlastest nõustus Eurobaromeetri uuringu väitega, et valitsus küsib aina rohkem isikuandmeid, Euroopa keskmine on kõrgem – 64% (Eurobaromeetri eriuuring 2011). Eesti inimesed kasutavad kõige aktiivsemalt tuludeklaratsiooni esitamist internetis ning digiretsepti, viimase kasutamist tõid, tõsi küll, aktiivselt välja ka need, kes end internetikasutajaks üldse ei liigitanud (eelkõige vanemaealised), seega ei räägi me tegelikult digiretsepti e-teenusena kasutamisest (TNS Emori uuring 2012). Eurobaromeetri andmekaitset ja privaatsust puudutava eriuuringu (Eurobaromeetri eriuuring 2011) põhjal võib aga öelda, et need enim kasutust leidvad valdkonnad on ühtlasi ka sellised, mida inimesed tajuvad kõige privaatsemana (nii Eestis kui ülejäänud Euroopas). Majandus- ja Kommunikatsiooniministeeriumi tellitud uuringu (TNS Emori uuring 2012) tulemustest võib näha, et inimeste rahulolematus e-teenustega on seotud pigem teenuse kasutamise keerukuse ja ajakuluga, kõige vähem toodi rahulolematuse põhjusena välja, et teenuse kasutamine ei ole turvaline (sh inimese privaatsuse jaoks). Andmete kogumise ja privaatsuse temaatika juures võibki Euroopas märgata teatud passiivsust, isegi fatalistlikku suhtumist, nii näiteks ütleb 74% Euroopa kodanikest, et isikliku info avaldamine on aina enam kaasaegse elu osa (Eurobaromeetri eriuuring 2011).

RIIKLIKE ANDMEKOGUDE TURVALISUSE PÕHIMÕTTED. Riiklikud andmekogud lähtuvad reeglina kolmest üldisest turvalisusega seonduvast põhimõttest, millest tulenevalt hinnatakse andmete turvalisuse taset ja määratakse turvalisuse nõuded: 1) konfidentsiaalsus (andmetele pääsevad ligi vaid volitatud isikud); 2) terviklikkus (andmed põhinevad algallikal, neid ei ole hiljem volituseta muudetud ja muudatused on jälgitavad) ning 3) kättesaadavus (andmed on õigel ajal ja mugavalt kättesaadavad ning kasutatavad) (Haas *et al.* 2011). Lisada võib vastutuse aspekti – inimeste õigus kriitikaks ning arupärimisteks (Fernández-Alemán *et al*. 2013). Nii tundlikku infot sisaldavad andmekogud on eriti ohustatud infolekete, viiruste ja andmevarguste suhtes. Eestis kasutusel oleva digitaalse terviseloo puhul on rakendatud eri meetmeid, mis muudaksid süsteemi turvaliseks ja läbipaistvaks. Näiteks jätavad kõik tegevused (nii andmete lisamine, muutmine kui ka vaatamine) maha jälje,

kahju tekitamiseks on vaja kompleksrünnet, puudub nn superadministraator, andmed on krüpteeritud ja siseneda saab ID-kaardi, mobiil-ID või muu sarnase vahendiga end autentides (Eesti e-tervise sihtasutus 2014).

FINANTSANDMED. Finantsandmete avaldamise all peetakse reeglina silmas igapäevapangandusega seonduvat, mis on küll suures osas eraettevõtete käes, kuid mida võib riigi tasandi kontrolli, levinud autentimisvahendina kasutamise ja mastaabi tõttu käsitleda ning tajuda ka riigi ja inimese suhtena. Võrreldes ELi keskmisega kasutavad eestlased agaralt internetipanganduse pakutavaid võimalusi (ELi keskmine näitaja on 47% kõigist internetikasutajatest, Eestis on see näitaja 69%). Eraldi küsimus Eurobaromeetri uuringus käsitles tuludeklaratsiooni esitamist ning muid e-teenuseid, kus on taas Euroopa keskmine (23%) palju väiksem Eesti kasutamispopulaarsusest (68%) (Eurobaromeetri eriuuring 2011).

ANDMETE KOMBINEERIMINE. Aina enam kombineeritakse ka erinevaid andmeid, seda nii suurte andmehulkade (nn *big data*) töötlejate jaoks kui ka inimeste endi kasutamiseks. Näiteks oli paar aastat tagasi iga teine Eesti internetikasutaja kasutanud riigiportaali eesti.ee (TNS Emori uuring 2012), mis koondab riigi- ja munitsipaalasutuste e-teenuseid, infot erinevate eluvaldkondade kohta ning asutuste kontaktandmeid. Kõikvõimalike registrite ning andmebaaside lisandumise ja täiustamise käigus peavad tänapäeva (demokraatlikud) riigid pöörama tähelepanu kodanike privaatsusega seonduvatele eri aspektidele. Näiteks inimeste **tervisest** kõneldes on oluline märkida, et Eesti on erakordne oma geenivaramu poolest (biopank, millega on vabatahtlikult liitunud ligi 5% Eesti täiskasvanud elanikkonnast), kuhu kogutud andmed võimaldavad läbi viia geneetikauuringuid ning mis on lähtealus personaalse meditsiini juurutamisele Eestis (Tartu Ülikooli Eesti Geenivaramu 2014). Personaalne meditsiin ja sellega kaasas käivad ülipõhjalikud tundlikke andmeid sisaldavad andmebaasid on aina enam arutletav teema ka privaatsusriskide puhul.

Internetiprivaatsust hõlmavad diskussioonid piirduvad sageli sõnavabaduse ja tsensuuri üle arutlemisega, kuid vahendatud avalikkuse püsivuse, kopeeritavuse, otsitavuse ja nähtamatule auditooriumile kättesaadavuse oludes on füüsilises maailmas lihtsamini kustuv ja kaduv info ka riikidele kättesaadav. Maailmas on viimasel ajal olnud mitmeid hoiatavaid näiteid selle kohta, kuidas riigid sekkuvad väga agressiivselt inimeste sõnavabadusse ja informatsioonilisse enesemääramisse, riivates sellega üksikisikute privaatsust: näiteks Indias võib ebasobiva sisu Facebookis laikimise eest saada 90päevase vanglakaristuse (Cooper 2014) ning Hiinas on valitsus palganud kaks miljonit inimest (nn avaliku arvamuse analüütikud), kes jälgivad muu hulgas seda, et inimesed ei postitaks valitsust kritiseerivaid arvamusavaldusi (Hunt 2013). Lähtuvalt kultuurilistest erinevustest näeme eri lähenemisviise ka lääne kultuurides – kui USAs on privaatsusega seonduvate probleemide (ise)reguleerimise eesotsas erasektor ning kodanikud näevad tihti ohuna oma privaatsusele riiki ja valitsust, kelle mõjuvõimu soovitakse kärpida (Belanger ja Hiller 2006), siis Euroopas, sealhulgas Eestis, nähakse privaatsust kaitsvaid reegleid sätestavat valitsust sageli kui usaldusväärset päästjat (Titiriga 2011, Eurobaromeetri eriuuring 2011).

TÖÖSUHTED

Avalikkuse ette on jõudnud mitu üksikisiku informatsioonililise privaatsuse ja töösuhetega seotud probleemset juhtumit. Välismaiste markantsete näidetena võib tuua välja, kuidas üks naine kirjutas Twitterisse, et ta vihkab oma tööd ja bossi, misjärel ülemus kirjutas vastupostituse: „Ära muretse. Sa oled vallandatud" (Dietrich 2013), või kuidas ühel arstil oli sotsiaalmeedia kaudu avalikult kättesaadav aastatetagune pilt, kus ta tudengina alkoholijoobes stripptantsu posti kallistas ning millest ajendatuna üks patsient kaebuse esitas (Sibicca ja Wesson 2012). Samuti on teada juhtum, kus juhtival kohal töötav inimene põhjendas töölt eemal viibimist vandekohtus osalemisega, kuid Facebooki profiililt nähtus, et ta oli hõivatud hoopis meelelahutuslikemate tegevustega (Slattery 2010). Eesti juhtumitest tasub meelde tuletada, kuidas pangatellerid Orkutis või mahlabaari teenindajad Facebookis kliente mõnitasid (Šmutov 2007, Tigas 2013), kuidas Tartu Ülikooli Kliinikumi intensiivraviosakonna õde pani Facebooki sureva lapse pildi koos endapoolse kirjeldusega oma tööst (Puuraid 2012) või kuidas Kaitseväe ohvitser sõimas Facebookis Afganistanis hukkunud Eesti kaitseväelast (Delfi 2012). Ühe Eesti ettevõtte töötaja kasutas oma blogis sõna „koodineeger", potentsiaalne välismaine äripartner ei mõistnud taustauuringut tehes selle sõna kasutamise konteksti ning loobus tehingust (Eslas ja Koch 2012). Selliste juhtumite taustal on hea analüüsida seda, kuidas töösuhte privaatne külg on segunenud avalikuga ja vastupidi – töötajad on rikkunud tööandja privaatsust ning tööandjad töötajate oma. Nagu näeme, on tekkinud uudsed ning reguleerimist vajavad olukorrad.

TAUSTAUURING TÖÖKOHALE KANDIDEERIMISEL. Kui inimene kandideerib töökohale, on üsna suur tõenäosus, et kogu info, mida ta on sotsiaalmeedias avalikult jaganud, jõuab ka tööandjani, kuid kontekstis, millisena see algselt plaanitud ei olnud (Nicolaisen 2010). Inimeste poolt sotsiaalmeedias tehtud avalike postituste, blogide ja e-kirjade tõttu on sagenenud juhtumid, kus töötaja eraelu tõttu kannatab tööelu ja ettevõtte avalik maine (Umphress *et al*. 2013), ja seetõttu on märgata värbajate ja personalijuhtide huvi pidevat suurenemist internetikeskkonnas tehtavate taustauuringute vastu. Stabiilselt väidab umbes 70% uuringutes osalenud personalijuhtidest, et nad kasutavad värbamisprotsessis sotsiaalmeediat ja on lükanud kandidaadi tagasi teabe (ebasobivad pildid, foorumipostitused jms) tõttu, mis internetipõhises taustauuringus esile kerkis (Rosen 2010, Preston 2011). Teisalt võib välja tuua, et läbimõeldud enesetutvustus sotsiaalmeedias, eriti Facebooki või LinkedIni keskkonnas, võib aidata kaasa töökoha leidmisele (Siibak ja Suder 2013).

Eestis on teemat uurinud Greete Kempel (2014), Eva-Liis Ivask (2013) ja Katriin Visamaa (2012), kes leidsid kõik samuti veenvaid tõendeid, et tööle kandideerija kohta internetis taustauuringu tegemine on muutunud tavapäraseks, hoolimata sellest, et tihtipeale võib selline teguviis tunduda privaatsuse rikkumisena. Kõige enamlevinum on kandidaadi kohta lisainformatsiooni otsimine Facebookist, kuid jälgitakse ka otsingumootorite (eelkõige Google) tulemusi ning teisi internetikeskkondi. Kandidaate reeglina eelnevalt taustauuringu tegemisest ei teavitata ning neilt kõnealuseks toiminguks nõusolekut ei küsita. Tööandjad peavad ebasobivaks sotsiaalmeedia kasutuseks näiteks ropendamist, seksuaalse alatooniga piltide üleslaadimist ja peopilte, aga ka tööandja-kolleegide mustamist ja tööalase konfidentsiaalse info lekitamist (Kempel 2014). Üsna tavaliseks võib pidada ka seda, kui kolleegid (hoolimata organisatsiooni võimuhierarhiast) on „sõbrad" sotsiaalmeediakeskkondades. Pinget lisavad olukorrad, kus sõbrakutse esitajaks on näiteks

ülemus või ettevõtte personalijuht. Globaalselt on teada ekstreemsemaid juhtumeid, kus tööintervjuudel küsitakse kandideerijalt nende Facebooki paroole või palutakse kontole sisse logida ja seejärel lasta ülemusel või värbajal seal ringi vaadata (van Dijck 2013, Roth *et al*. 2013).

ÕIGUSLIK REGULATSIOON. Kempel (2014) toob välja, et Eesti Vabariigi seadusandlusest ei saa sotsiaalmeedia küsimuses erilist tuge: piiritletud on eraelu puutumatuse mõiste, samuti sätestatakse, et isikuandmete mistahes töötlemise korral tuleb andmesubjekti teavitada, kuid sotsiaalmeedia kohta käiv tuleb välja lugeda ridade vahelt ning esineb palju vastuolulisi ettekirjutusi. Tööandja justkui ei tohiks (potentsiaalse) töötaja isikuandmeid ilma nõusolekuta töödelda, kuid tõendite ja kontrollita on selle takistamine võimatu (Siibak ja Suder 2013).

ÄRISUHTED

B2C KAUBANDUS: INTERNET JA KLIENDIKAARDID. Ärisuhetest kõneldes tasub eristada e-teenuseid ja e-kauplemist võimaldavaid ärisuhteid (eelkõige veebipoed) ning internetisisu pakkujaid (eelkõige Facebook ja Google). Riigikantselei 2013. aastal valminud uuringust selgus, et 86% uuringus osalenud Eesti kodanikest on ostnud kaupu või teenuseid e-kanalitest (Riigikantselei 2013); 2013. aasta kevadel teostatud Eurobaromeetri uuringu järgi ostles internetis viimase 12 kuu jooksul 46% eestlastest vanuses 15+ (Eurobaromeetri eriuuring 2013), TNS Emori uuringus lisandus veel mõni protsendipunkt – 49% (Voog 2014). Inimestele võib e-kauplemisel pakkuda lisakindlust ja julgust see, et internetis on võimalik rahulolematutel tarbijatel kiiresti ja lihtsalt kaebusi esitada, samuti on tarbijal ärisuhetes suurem võim kui varem, kuna ettevõtjad pelgavad negatiivsete ostukogemuste levikut sotsiaalmeedias (Jasper ja Waldhart 2013). Kuid ei maksa unustada ka füüsilises ruumis asuvaid kaupluseid, mis samuti koguvad inimeste kohta infot. Poed kasutavad laialdaselt kliendikaardisüsteemi ning eestlased on agarad sooduskaartide kasutajad – 71% eestlastest väitis end mõnda kliendikaarti kasutavat, samas kui näiteks Euroopa keskmine näitaja on tunduvalt madalam, 47% (Eurobaromeetri eriuuring 2011). Inimese **ostuharjumuste** põhjal on võimalik tema kohta palju teada saada. Üks kurioossemaid näiteid pärineb USAst, kus kaubanduskett Target analüüsis ennustava statistika abil põhjalikult oma klientide oste, et selle põhjal teada saada, kes on tõenäoliselt raseduse viimases trimestris, mil ostuharjumused on muutumas paindlikumaks (Duhigg 2012). Ühe juhtumi puhul saatis Target rasedus- ja beebitoodete reklaame ning kuponge noorele tüdrukule ning seeläbi said rasedusest teadlikuks ka tema teised pereliikmed. Kõnealune juhtum liigitati avaliku arutelu käigus tõsise privaatsuse rikkumise alla, kuid ettevõtted rõhutavad, et kui isik soovib kaitsta oma privaatsust (näiteks piirates juurdepääsu oma infole, kitsendades enda jälgimise võimalusi või jagades infot minimaalselt, rakendades õigust olla rahule jäetud), siis jääb ta ka ilma personaliseeritud kogemusest (Titiriga 2011).

PERSONAALSED PAKKUMISED. Erinevate teenuste pakkujad on huvitatud personaalsete pakkumiste tegemisest. Üks levinumaid võimalusi on käitumuslik suunatud pakkumine (Titiriga 2011), mida võiks käsitleda ka kui massidele stereotüübi alusel pakkumiste tegemisena (veebis nähtavaid valikuid ja pakkumisi mõjutab näiteks sugu, vanus, asukoht jne). Üks parimaid näiteid on Google AdWords, mille abil jälgitakse seda, mida kasutaja otsib

ja millel ta klikib ning sellest lähtuvalt kuvatakse erinevaid sponsoreeritud postitusi. Üks efektiivseimaid suunatud pakkumiste tegemise viise aga põhineb filtritel, mille aluseks on paljude teiste sarnaste või seotud kasutajate valikud (*collaborative filtering recommendation system*). Kui Google AdWordsi lingil klikkimise tõenäosus on keskmiselt 1%, siis kasutaja (ja tema sõprade) profiili arvesse võttev kontekstitundlikum soovitussüsteem tõstab tõenäosuse 3–4%-le (Titiriga 2011), mis on ka üks peamisi põhjuseid, miks Google lõi oma suhtlusvõrgustiku Google+.

ISIKLIKU INFO JAGAMISE PÕHJUSED. Miks peaks aga inimene enda ja oma sõprade kohta nii palju infot andma? Äri puhul on oluline tajutav kasu või teenusepakkuja-tarbija vahetuskaup ehk **lõivsuhe** (*trade-off*). Kõige tavalisem lõivsuhte motivatsioon on seotud üldise toote või teenuse tarbimisega – selleks et mingit veebikeskkonda üldse kasutada, peab enda kohta infot andma. Sellele järgneb veel üks samm – et inimene saaks teenust või toodet mugavamalt või tõhusamalt tarbida, peab ta andma enda kohta rohkem infot. Personaliseeritud veebikasutuse võimalus on eriti laialdaselt kasutusel sotsiaalvõrgustikes (Facebook, Instagram, Pinterest jne), kus kasutaja jätab endast sõbrasuhete, meeldimiste, jälgimiste, soovituste ja gruppidesse kuulumisega maha enda huvisid näitava digijälje. Privaatsust käsitleva Eurobaromeetri eriuuringu (2011) tulemustest saabki välja tuua, et kõige olulisem põhjus, miks inimesed enda kohta infot avaldavad, on eesmärk kasutada mingit teenust, seda nii sotsiaalvõrgustike (61%) kui ka e-kaubanduse puhul (79%).

ÜLISUURTE TEENUSEPAKKUJATE ERIJUHTUMID. Eelkõige on avalikkuse kõrgendatud tähelepanu all olnud kaks internetihiidu – Facebook ja Google. Facebooki vastu suunatud etteheited on seotud kasutajate teadliku nõusolekuta nende privaatse informatsiooni jagamisega kolmandatele osapooltele (MacMillan 2010) – kaubanduslikele organisatsioonidele ning reklaamivõrgustikele, et andmete ja nende alusel tehtavate pakkumistega tulu teenida (Youn 2009). Ka võib diskuteerida „teadlikkuse" aspekti üle, näiteks kui Google ühtlustas 2012. aastal oma eri teenuste ja platvormide privaatsuspoliitikaid ning viis sellega seoses kasutajatingimustesse sisse suuri muudatusi, ei teadnud enamik (90%) inimestest sellest midagi, ehkki info oli tehtud kättesaadavaks (Moscaritolo 2012). Inimeste jaoks on mitteotsustamine (kas olen kasutamistingimustega nõus) tehtud lihtsaks, uued tingimused rakenduvad isegi ilma teadliku nõusolekuta, seega on kasutajad muutunud ka passiivsemaks.

TEISED INIMESED ÜKSIKISIKU AVALIKU KUVANDI KUJUNDAJANA

Inimese enda, riigi, töösuhete ja ärisuhete kõrval võib ohustada üksikisiku privaatsust ka teine inimene, näiteks sõber või tuttav. Katrin Laas-Mikko (2010) on rõhutanud, et **privaatsusele on omane sotsiaalne loomus**, et ilma teiste olemasoluta ei ole ka privaatsusel väärtust. „Teised" osalevad uue meedia keskkondades aktiivselt meie identiteedi ja maine loomises. Kõige aktiivsem roll on muidugi inimesel endal, kasutajad saavad luua endale eri keskkondades tasuta profiilid, millele on võimalik lisada rohkelt fotosid ja videoid, märkida üles oma huvid, kontaktandmed, poliitilised vaated, seksuaalne sättumus, suhtestaatus ja palju muud infot. Fotodel ja videotes saab sildistada ehk *tag*'ida nendel

kujutatud inimesi, kelle profiilidele need fotod ja videod seeläbi ilmuvad, mistõttu võib väita, et näiteks inimese Facebooki-imago on teatud mõttes kollektiivne looming. Uurijad (Walther *et al*. 2008) on välja toonud, et see on isiku kuvandi kujundamise juures problemaatiline, kuna isikul ei ole teiste postitatava sisu üle erilist kontrolli, küll aga mõjutab teiste lisatud sisu potentsiaalselt lehekülje omanikust jäävat muljet. Kui isegi kasutaja ise peopilte üles ei lae, siis võivad seda teha tema sõbrad, mis aga tähendab samuti ohtu privaatsusele (McLaughlin ja Vitak 2012).

INTERNETI-KIRJAOSKUS JA -PRIVAATSUS. Privaatsust võivad rikkuda inimene ise või teised inimesed puudulike teadmiste tõttu. Interneti-kirjaoskus hõlmab endas väga erinevaid oskusi (näiteks info otsimine, info kriitiline hindamine, teenuste kasutamine, turvasätete rakendamine, netikett, kaasarääkimine jne), millele aga uurijate hinnangul ei ole kodanikuhariduses piisavalt tähelepanu pööratud, „tegude tasandil on enam tähelepanu pööratud infotehnoloogilise infrastruktuuri loomisele" (Runnel 2010). Reguleerijate ja seadusandjate jaoks on lihtne näha vastutavana (nii oma digitaalse kirjaoskuse kui privaatsuse eest) inimest ennast ning rahvas on selle ka omaks võtnud. Erinevates võimalikes privaatsust riivavates olukordades peetakse aktiivseks vastutajaks inimest ennast (Eurobaromeetri eriuuring 2011). Lisaks tuleb inimestel arvestada sellega, et kohaldatavad privaatsusnormid ei ole mitte kunagi universaalsed ning seetõttu sõltub iga inimese privaatsuse rikkumine konkreetsest situatsioonist – see, mis ühe jaoks on avalik, on teise jaoks privaatne (Siibak ja Suder 2013) ning reeglina tulevad need erinevad arusaamad välja konfliktses olukorras, kus keegi tajub oma privaatsuse rikkumist.

PRIVAATSUSE KAITSMISE VÕIMALUSED JA PIIRANGUD. Privaatsuse kaitsmisega seoses räägitakse Euroopas ka õigusest olla unustatud, õigemini kitsendatult õigusest kustutamisele, *right to erasure* (Euroopa Parlament 2014), kuid sellise lahenduse efektiivsuses võib kahelda, kuna internetis oleva info üks põhiomadus on kopeeritavus. Info võib olla juba mitmel moel ja väga paljudesse kanalitesse edasi levinud, näiteks saadavad võrgustikus olevad inimesed häbistava sisuga sotsiaalmeedia postitusest tehtud kuvatõmmise just sellisele sisule keskendunud lehekülgedele (nagu Lamebook või Failbook), sealt jagatakse ja kopeeritakse seda edasi erinevates blogides, tihti kopeerib selle automaatselt parasiitlehekülg, mõnikord jõuavad kurioossed näited eri riikide meediaväljaannete *online*-uudistesse või koguni teaduslikesse analüüsidesse, raamatutesse jne.

EESTLASTE PRIVAATSUSEGA SEONDUVAD HOIAKUD JA PRAKTIKAD VÕRRELDES EUROOPAGA

Nagu juba eespool korduvalt viidatud, avaldati 2011. aastal Euroopa Liidu liikmesriikide seas läbi viidud suuremahulise ja oma põhjalikkuse ja ülevaatlikkuse poolest unikaalne ning antud kontekstis oluline andmekaitset ja privaatsust käsitlev Eurobaromeetri eriuuring (Eurobaromeetri eriuuring 2011). Üks käesoleva uuringu läbiviimise motivatsioone oli muu hulgas ka asjaolu, et Eurobaromeetri andmed koguti 2010. aastal ning võttes arvesse vahepeal toimunud privaatsusega seonduvaid skandaale ja veebivaldkonna arengut, on

olemas vajadus uuemate andmete järele. Alljärgnevalt on välja toodud mõned olulisemad aspektid eestlaste kohta võrreldes Euroopaga.

Kõige enam peavad eestlased privaatseks (vt tabel 1) enda isikut identifitseerivate dokumentide andmeid (isikukood, ID-kaardi ja passi andmed), seejärel enda meditsiiniandmeid, oma finantsandmeid (mille all peetakse silmas eelkõige palga suurust), krediitkaardi ajalugu ja pangakonto andmeid.

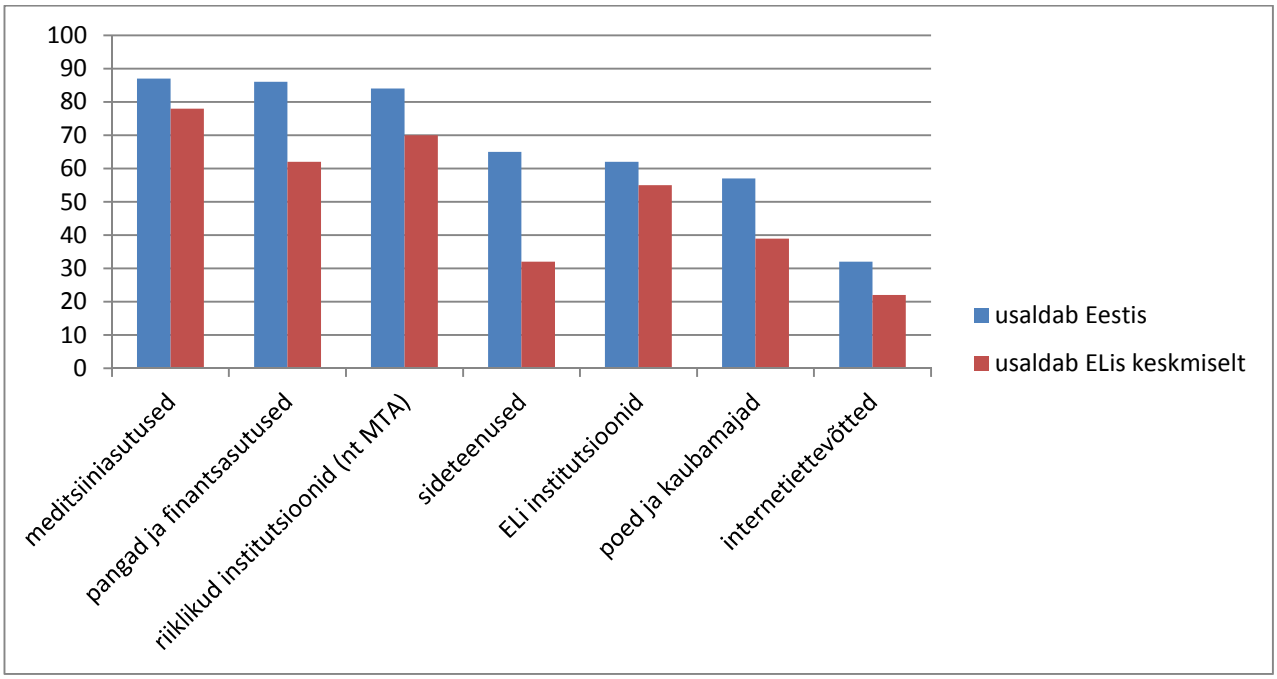
Tabel 1. Mida peetakse privaatseks infoks – Eesti võrdlus Euroopa keskmisega (Allikas: Eurobaromeetri eriuuring 2011)

Valdkond	Peab privaatseks Eestis	Peab privaatseks ELis keskmiselt
Isikukood, ID-kaardi ja passi andmed	85%	73%
Meditsiiniandmed	81%	74%
Finantsandmed	79%	75%
Sõrmejäljed	66%	64%
Kodune aadress	58%	57%
Mobiiltelefoninumber	54%	53%
Nimi	44%	46%
Fotod endast	41%	48%
Kes on sõbrad	22%	30%
Rahvus	22%	26%
Tööga seonduv teave	19%	30%
Isiklikud arvamused ja eelistused	19%	27%
Tegevused (hobid, sport, tegevuskohad)	18%	25%
Veebilehed, mida külastatakse	18%	25%

Üldreegel on, et **mida kõrgem on hariduslik ja sotsiaal-majanduslik staatus, seda enam privaatseks hindavad eurooplased enda kohta käivat infot üldisemalt**.

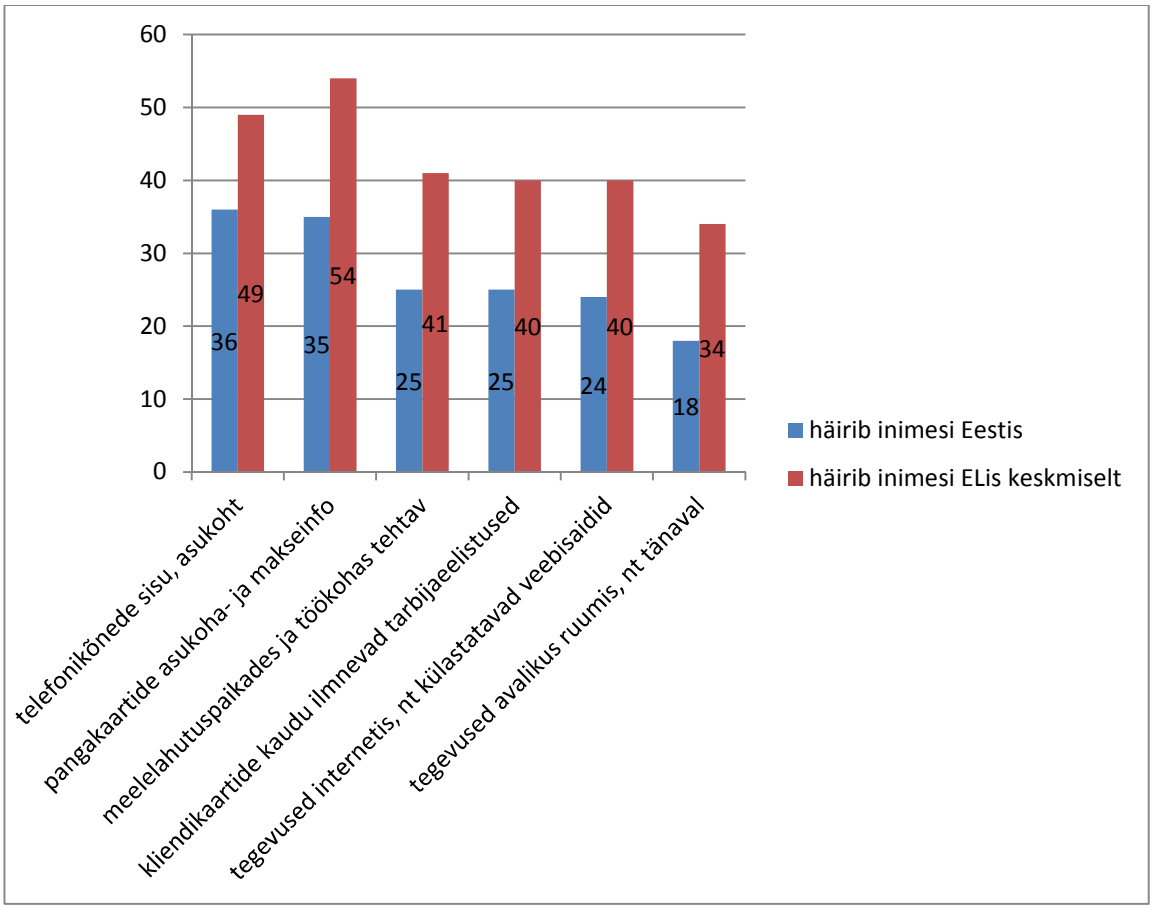
Privaatsusega seonduvates hoiakutes on palju leplikkust või isegi passiivset alistumist: 77% eestlastest nõustub väitega, et enda kohta info avaldamine on tänapäeval aina olulisem ja levinum (Euroopa keskmine 72%); arvatakse ka, et isikuandmete avaldamisest ei ole pääsu, kui soovitakse teatud teenuseid ja tooteid tarbida (Eesti 54%, EL 58%). Lisaks ei pea 47% eestlastest isikliku info avaldamist üldse küsimuseks või probleemiks, eurooplased keskmiselt on ettevaatlikumad ja umbusaldavamad, 33% eurooplastest ei pidanud isikliku info avaldamist probleemiks.

Eestlased paistavad silma on kõrge usaldusmääraga väga paljudes küsimustes: eestlased usaldavad Euroopa keskmisest tunduvalt enam nii riiki ja avalikku sektorit kui ka erasektorit, nii panku kui ka internetiühenduse pakkujaid (vt joonis 2).



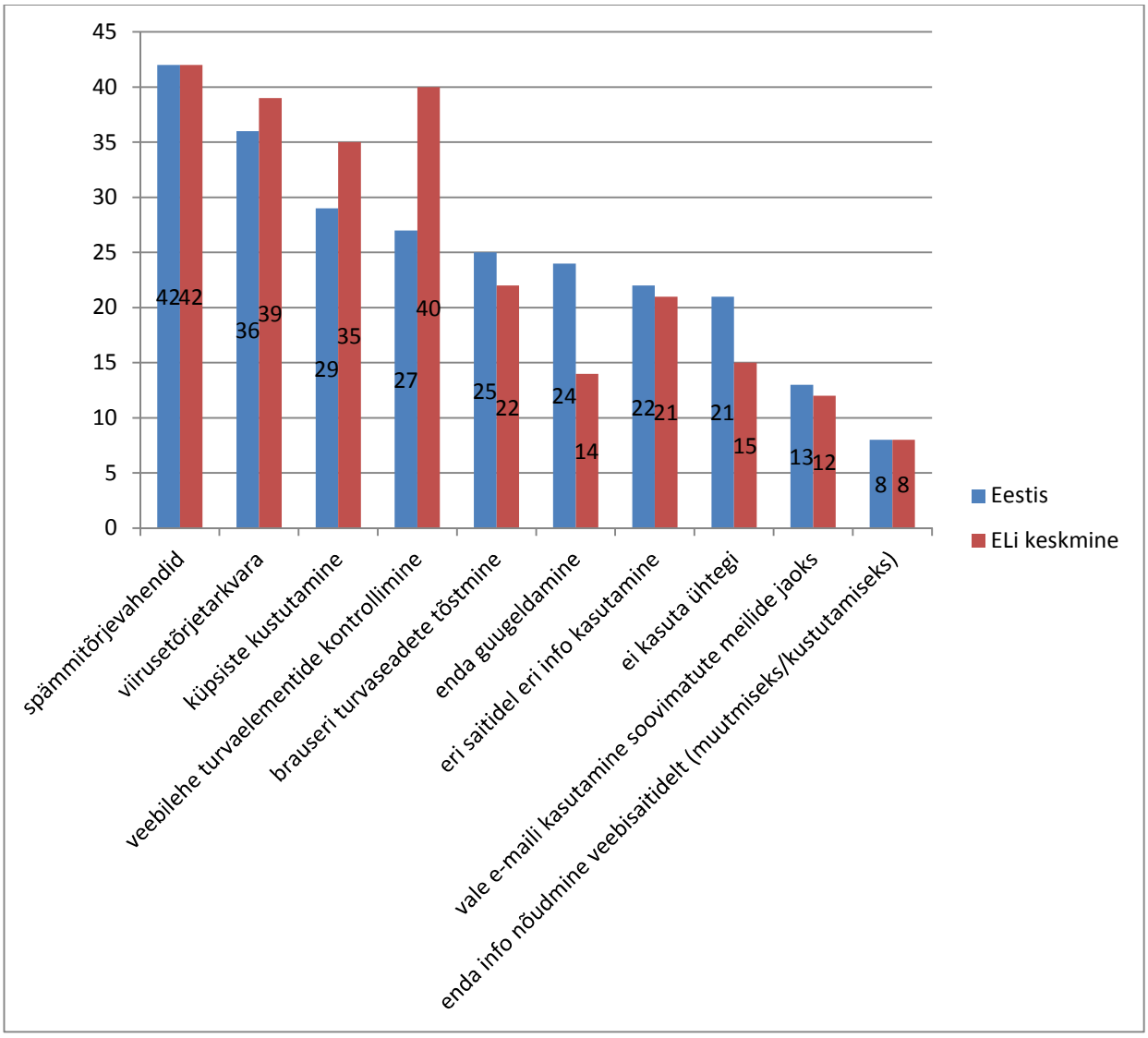
Joonis 2. Institutsioonide usaldus Eestis ja Euroopas keskmiselt (Allikas: Eurobaromeetri eriuuring 2011)

Üldiselt tunnevad Eesti inimesed võrreldes ülejäänud Euroopaga vähem häiritust ja muret oma andmete kogumise ja salvestamise pärast (vaata joonis 3), stabiilselt kõigis kategooriates on Eesti näitajad umbes 15% väiksemad Euroopa keskmisest. Niisamuti ei muretse meie inimesed oma andmete kasutamise pärast teistel eesmärkidel, kui neid algselt kogutakse (Eestis mures 51%, Euroopas keskmiselt 70%); vaid rootslased on selles küsimuses meist muretumad.



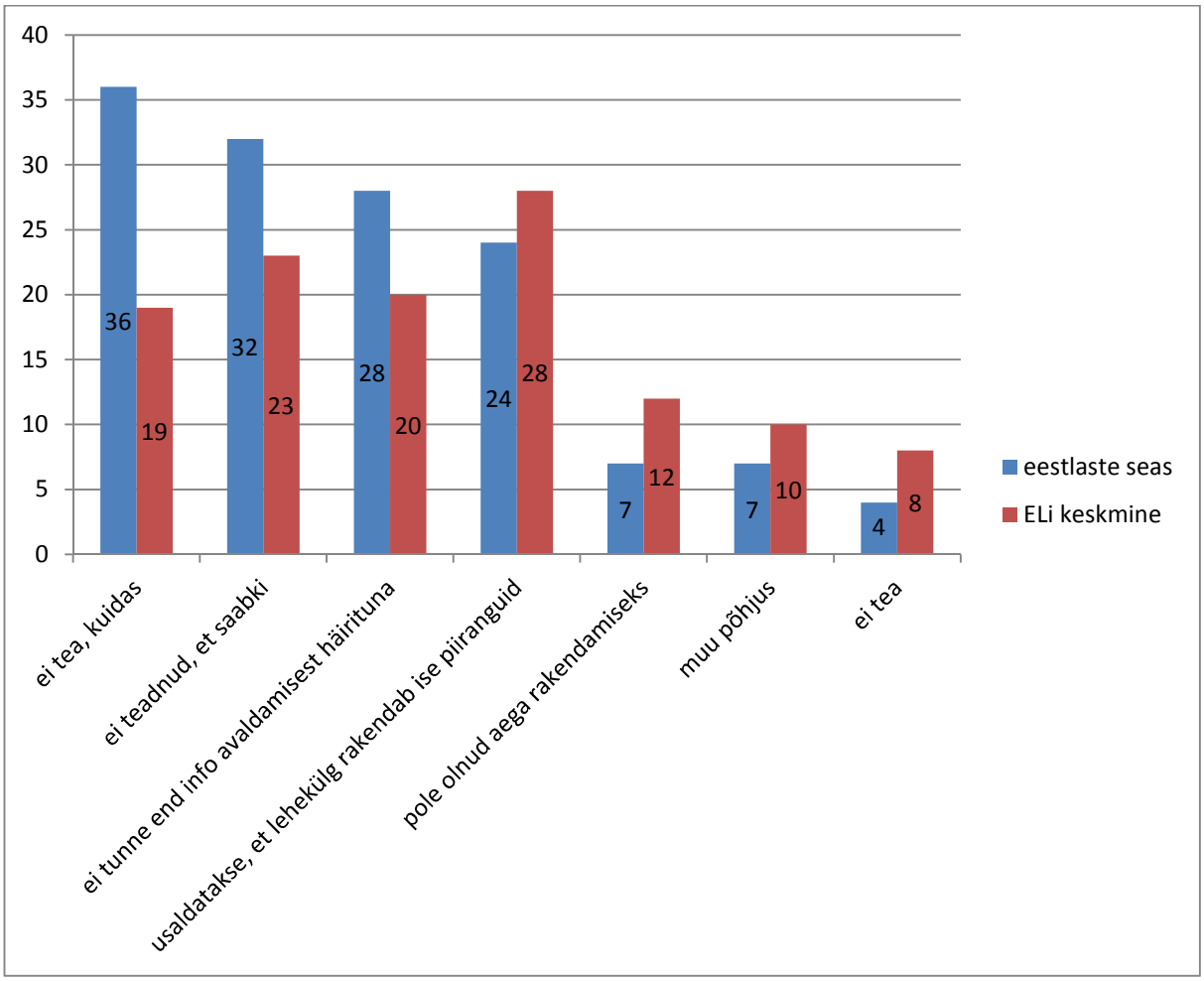
Joonis 3. Eestlaste häiritus erinevate tegevuste jälgimise puhul võrreldes Euroopa keskmisega (Allikas: Eurobaromeetri eriuuring 2011)

Eestlased kasutavad Euroopa keskmisest vähem kõikvõimalikke privaatsust ja identiteeti kaitsvaid strateegiaid ning tööriistu (vt joonis 4). Tuleb märkida, et Eurobaromeetri uuringus on vastusevariantidena esitatud võimalused piiratud ja loetelu mittetäielik. Ometi võib tulemustes märgata, et eestlased väidavad end kasutavat eelkõige tehnilisi, mitte sotsiaalseid strateegiaid ja tööriistu.



Joonis 4. Eestlaste poolt oma identiteedi (ja privaatsuse) kaitsmiseks internetis kasutatavad strateegiad ja tööriistad võrreldes Euroopa keskmisega (Allikas: Eurobaromeetri eriuuring 2011)

Kõige enam peavad küsitletud eurooplased info eest vastutavaks inimest ennast. Inimese vastutus oma privaatsuse kaitsmisel on seotud näiteks teadlikkuse ja tegevuse läbimõeldusega. Võime märgata, et vajalike teadmiste puudumist tunnistavad eestlased Euroopa keskmisest sagedamini. 54% eestlastest loeb küll läbi erinevate teenuste privaatsus- ja kasutamistingimused, mis on üsna sarnane Euroopa keskmisega (58%), kuid erinevus tekib vastusevariandis „ma ei tea, kust neid leida" – Eesti inimesed vastasid nii 10% juhtudest, mis on Euroopa riikide seas kõrgeim näitaja (Euroopa keskmine 5%). Eestlastest sotsiaalmeedia kasutajad kasutavad võrreldes Euroopaga keskmiselt agaramalt keskkondade privaatsusseadete muutmist endale sobivaks (60% *vs*. 51%) ning peavad seda lihtsaks (90% eestlastest sotsiaalmeediakasutajatest, kes on seadeid muutnud; ELi keskmine 82%). Nende sotsiaalmeediakasutajate hulgas aga, kes ei ole privaatsusseadeid muutnud, on eestlased taas Euroopas esikohal vastusega „ma ei tea, kuidas seda teha", kõrge vastanute protsent on ka vastuse „ma ei teadnud, et seda saab teha" puhul (vt joonis 5).



Joonis 5. Põhjused, miks privaatsusseadeid ei rakendata. Eestlaste ja Euroopa keskmiste näitajate võrdlus nende sotsiaalmeediakasutajate seas, kes ei ole privaatsusseadeid muutnud (Allikas: Eurobaromeetri eriuuring 2011)

Viimases tabelis välja toodu tõendab seega veel kord, kuivõrd oluline on üksikisiku enda digitaalse kirjaoskuse ja digitaalsete pädevuste arendamine, kuid ka seda, et seni kuni need oskused on piiratud, ei ole kõige otstarbekam jääda lootma üksikisiku vastutusele.

KOKKUVÕTE

Uuringu käesoleva osa eesmärk on anda ülevaade privaatsuse mõiste ja sellega seotud arutelu kohta, kirjeldada võimalikke tajutavaid privaatsuse riiveid eri kontekstides ning tutvustada eestlaste hoiakuid võrreldes keskmise eurooplasega.

Uuringus käsitletakse eelkõige informatsioonilist privaatsust ehk informatsioonilist enesemääramist, mis hõlmab inimese kohta kogutud, salvestatud ja jagatud andmeid. Privaatsuse kontseptsioon on kompleksne ning selle sisu määratlemine palju tuliseid vaidlusi tekitanud. Privaatsusõigus annab üksikisikule õiguse otsustada, kes ja mil määral saab juurdepääsu teda puudutavale informatsioonile ja kasutada seda teavet. Käesolevas uuringus vaadeldakse, milliseid olukordi inimesed tajuvad privaatsetena ja potentsiaalselt privaatsust rikkuvatena. See, mida tajutakse privaatsena, sõltub ja on mõjutatud kontekstist.

Info- ja kommunikatsioonitehnoloogia kiire areng on muutnud meie igapäevaelu: laiendanud kasutusvõimalusi, suurendanud liikuvust, kasutajate hulka, sotsiaalseid käitumistavasid ja -norme. Uus meedia on seganud kokku erinevad ja seni eraldatud auditooriumid ja kontekstid, ähmastanud piire avaliku ja eraelu vahel. Samas loovad uued tehnoloogiad ja keskkonnad ka uusi lahendusi ning võimaldavad erinevaid *online*-strateegiaid privaatsuse säilitamiseks – alates tagasihoidlikust teabe kasutusest ja enesetsensuurist kuni keerukamate strateegiateni, nagu sotsiaalne steganograafia ja mitme identiteedi või pseudonüümide kasutamine.

Kuigi mõned skeptikud on väljendanud arvamust, et „privaatsus on surnud", on siiski avalikkuse ja teadusringkondade vaidlustes rõhutatud privaatsuse kaitsmise vajadust. Selles aga, miks privaatsuse kaitsmine on soovitatav, ei ole üksmeelele jõutud. Kuid arvatakse, et privaatsuse peamine ülesanne on kaitsta üksikisiku autonoomiat ja mina-pildi arengut. Privaatsus annab meile otsustusõiguse kujundada oma elu ja kuvandit endast ning kaitsta seda teiste sekkumise eest. Privaatsus teeb võimalikuks tähenduslike suhete loomise teistega, kuna võimaldab sotsiaalsetel toimijatel tõmmata piiri enda ja teiste vahele ja olla sotsiaalseks suhtlemiseks suletud või avatud sõltuvalt kontekstist.

Eristada saab kuut peamist privaatsuse riivamise viisi: puudulik teavitamine, kasutuseesmärgile mittevastamine, nõusoleku puudumine, turvaaugud ja infolekked, piiratud juurdepääs (isiku) enda andmetele ja andmekogujate vastutuse puudumine. Privaatsuse tajumine sõltub eri kontekstidest ja neid kontekste defineerivatest suhetest. Uuringus käsitletakse privaatsusega seonduvaid probleeme neljas järgmises suhete valdkonnas: 1) riigi ja inimese vahelised suhted; 2) töösuhted; 3) ärisuhted ning 4) suhted teiste inimestega.

Uuringu käesolevas osas on toodud välja ka eelnevatest avaliku arvamuse uuringutest selgunud eestlasi iseloomustavad hoiakud võrreldes muude Euroopa liikmesriikide elanikega. Üldiselt tunnevad eestlased end vähem häirituna ja muretsevad vähem oma andmete kogumise pärast. Eestlaste hoiakut iseloomustab leplikkus ja isegi passiivne suhtumine informatsiooni avaldamisse. Eestlased nõustuvad sagedamini väitega, et enda kohta andmete

avaldamine on tänapäeval aina olulisem. Samuti arvatakse, et isiklike andmete avaldamisest ei ole pääsu, kui soovitakse teatud teenuseid ja tooteid tarbida. Eestlasi iseloomustab ka Euroopa keskmisest kõrgem usaldus nii avaliku kui ka erasektori vastu andmete töötlemisel. Kuid nagu eurooplased üldiselt, peavad ka eestlased info kaitsmise eest vastutavaks inimest ennast. Samas tunnistavad eestlased vajalike teadmiste puudumist sagedamini kui Euroopas keskmiselt.

KIRJANDUS

1. Albrechtslund, A. (2008). Online Social Networking as Participatory Surveillance. *First Monday*, 13(3). URL: http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/viewArticle/2142/1949
2. Altman, I. (1975). *The Environment and Social Behavior: Privacy, Personal Space, Territory and Crowding*. Monterey, California: Brooks/Cole.
3. Baghai, K. (2012). Privacy as a Human Right: A Sociological Theory. *Sociology*, 46(5), lk 951–965.
4. Belanger, F.; Hiller, J. (2006). A Framework for E-Government: Privacy Implications. *Business Process Management Journal*, 12(1), lk 48–60.
5. Bennett, C. J. (1971). *Regulating Privacy: Data Protection and Public Policy in Europe and the United States*. Ithaca, N.Y.: Cornell University Press.
6. Bovill, M.; Livingstone, S. (2001). Bedroom Culture and the Privatization of Media Use. Livingstone, S. and Bovill, M. (toim). *Children and their Changing Media Environment. A European Comparative Study*. New Jersey: Lawrence Erlbaum Associates, Inc. Lk 113–140.
7. boyd, d. m. (2007). Social Network Sites: Public, Private, or What? *Knowledge Tree 13*. URL: http://www.zephoria.org/thoughts/archives/2007/05/07/social_network-3.html
8. boyd, d. m. (2008). *Taken Out of Context: American Teen Sociality in Networked Publics*. Doktoritöö. University of California, Berkeley. URL: http://www.danah.org/papers/TakenOutOfContext.pdf
9. boyd, d. m. (2010). Social Steganography: Learning to Hide in Plain Sight. *danah boydi blogi,* 23. august. URL: http://dmlcentral.net/blog/danah-boyd/social-steganography-learning-hide-plain-sight
10. boyd, d.; Marwick, A. (2011). Social Steganography: Privacy in Networked Publics. *Ettekanne. International Communication Associationi konverents.* Boston, MA. URL: http://www.danah.org/papers/2011/Steganography-ICAVersion.pdf
11. Brin, D. (1998). *The Transparent Society.* Reading, MA: Perseus Books.
12. Cooper, D. (2014). India Makes 'Liking' Blasphemous Content Illegal*. Engadget.com*, 22. august. URL: http://www.engadget.com/2014/08/22/india-censorship-blasphemy-laws-digital/
13. Craig, T.; Ludloff, M. E. (2011). *Privacy and Big Data: The Players, Regulators, and Stakeholders.* Sebastopol: O'Reilly Media.
14. Davis, F. D. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. *MIS Quarterly*, 13(3), lk 319–340.
15. Dietrich, G. (2013). Social Media Policy: When Are Your Own Opinions Not Okay? *Social Media Today*, 26. september. URL: http://socialmediatoday.com/ginidietrich/1765916/social-media-policy-when-are-your-own-opinions-not-okay
16. van Dijck, J. (2013). You Have One Identity: Performing the Self on Facebook and LinkedIn. *Media, Culture & Society*. 35(2), lk 199–215.
17. Duhigg, C. (2012). How Companies Learn Your Secrets. *The New York Times*, 16. veebruar. URL: http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=1&_r=1&hp&pagewanted=all
18. Eslas, U.; Koch, T. (2012). Sõna «neeger» seadis ohtu tööpakkumise. *Postimees,* 1. november. URL: http://www.postimees.ee/1025662/sona-neeger-seadis-ohtu-toopakkumise
19. Fernández-Alemán, J. L.; Señor, I. C.; Lozoya, P.A.O.; Toval, A. (2013). Security and Privacy in Electronic Health Records: A Systematic Literature Review. *Journal of Biomedical Informatics*, 46(3), lk 541–562.

20. Foucault, M. (1991). *Discipline and Punish: The Birth of the Prison*. London etc: Penguin Books.
21. Fried, C. (1984). Privacy. Schoeman, F. D. (toim). *Philosophical Dimensions of Privacy: An Anthology.* Cambridge: Cambridge University Press, lk 203–222.
22. Garfinkel, S. (2001). *Web Security, Privacy and Commerce*. Sebastopol, CA: O'Reilly.
23. Gavison, R. (1980). Privacy and the Limits of Law. *The Yale Law Journal*, 89(3), lk 421–471. URL: http://courses.ischool.berkeley.edu/i205/s10/readings/week11/gavison-privacy.pdf
24. Gross, H. (1967). The Concept of Privacy. *New York University Law Review*, 42, lk 34–53.
25. Haas, S.; Wohlgemuth, S.; Echizen, I.; Sonehara, N.; Müller, N. (2011). Aspects of Privacy for Electronic Health Records. *International Journal of Medical Informatics*, 80(2), lk 26–31.
26. Hunt, K. (2013). China 'Employs 2 Million to Police Internet'. *CNN Asia*, 7. oktoober. URL: http://edition.cnn.com/2013/10/07/world/asia/china-internet-monitors/
27. Ivask, E-L. (2013). *Facebooki kasutamine tööle kandideerijate taustauuringu tegemisel teenindussektori asutuste näitel*. Bakalaureusetöö, juh. A. Siibak, Tartu Ülikool, ajakirjanduse ja kommunikatsiooni instituut. URL: http://dspace.utlib.ee/dspace/handle/10062/31312
28. Jasper, C. R.; Waldhart, P. (2013). Internet and Distance Channel Use and European Consumer Complaint Behavior. *The International Review of Retail, Distribution and Consumer Research*, 23(2), lk 137–151.
29. Kalvet, T.; Tiits, M.; Hinsberg, H. (2013). *E-teenuste kasutamise tulemuslikkus ja mõju*. Tallinn: Balti Uuringute Instituut ja Poliitikauuringute Keskus Praxis. URL: http://www.ibs.ee/et/publikatsioonid/item/116-e-teenuste-kasutamise-tulemuslikkus-ja-moju
30. Kempel, G. (2014). *Sotsiaalmeedia töösuhtes: tööandjate hinnangud ning kogemused*. Magistritöö, juh. A. Siibak, Tartu Ülikool, ühiskonnateaduste instituut. URL: http://dspace.utlib.ee/dspace/handle/10062/42383
31. Kirkpatrick, M. (2010). Facebook's Zuckerberg Says the Age of Privacy is Over. *Readwrite*, 9. jaanuar. URL: http://www.readwriteweb.com/archives/facebooks_zuckerberg_says_the_age_of_privacy_is_ov.php
32. Knibbs. K. (2013). In the Online Hunt for Criminals, Social Media is the Ultimate Snitch. *Digital Trends*, 13. juuli. URL: http://www.digitaltrends.com/social-media/the-new-inside-source-for-police-forces-social-networks/#!bNLp76
33. Kupfer, J. (1987). Privacy, Autonomy, and Self-concept. *American Philosophical Quarterly*, 24: 1, lk 81–89.
34. Laas-Mikko, K. (2010). *Privaatsuse filosoofilise kontseptsiooni piiritlemine.* Magistritöö, juh. M. Sutrop, Tartu Ülikool, Filosoofia ja semiootika instituut. URL: http://dspace.utlib.ee/dspace/bitstream/handle/10062/15048/laas-mikko_katrin.pdf?sequence=1
35. Larsen, M. C. (2007). 35 Perspectives on Online Social Networking. *Social Computing Magazine*, 5. juuli. URL: http://vbn.aau.dk/files/17515817/35_Perspectives_on_Online_Social_Networking_by_Malene_Charlotte_Larsen.pdf
36. Linaa Jensen, J. (2010). The Internet Omnopticon - Mutual Surveillance in Social Media. *Ettekanne. Internet Research 11.0: Sustainability, Participation, Action*. Gothenburg, Rootsi, 19.–21. oktoober 2010.
37. McLaughlin, C.; Vitak, J. (2012). Norm Evolution and Violation on Facebook. *New Media Society*, 14(2), lk 299–315.
38. MacMillan, D. (2010). Facebook's Washington Problem. *Businessweek*, 17. mai, lk 33–34.
39. Marwick, A. E.; Murgia-Diaz, D.; Palfrey, J. G. (2010). Youth, Privacy and Reputation (Literature Review). *Berkman Center Research Publication No. 2010-5; Harvard Public Law Working Paper No. 10-29*. URL: http://ssrn.com/abstract=1588163

40. Mathiesen, T. (1997). The Viewer Society: Michel Foucault's "Panopticon" Revisited. *Theoretical Criminology,* 1(2), lk 215–234.
41. Mayes, T. (2011). We Have No Right to Be Forgotten Online. *The Guardian*, 18. märts. URL: http://www.theguardian.com/commentisfree/libertycentral/2011/mar/18/forgotten-online-european-union-law-internet
42. Miller, A. R. (1971). The Assault on Privacy: Computers, Data Banks and Dossiers. Ann Arbor: University of Michigan Press.
43. Moore, A. (2008). Defining Privacy. *Journal of Social Philosophy*, 39, lk 411–428.
44. Moscaritolo, A. (2012). Most Users In the Dark About Google's New Privacy Policy. *PC Magazine*, veebruar.
45. Nergi, A. (2013). Facebooki konto kaudu saab hinnata laenaja maksevõimet. *Eesti Päevaleht*, 8. mai. URL: http://arileht.delfi.ee/news/uudised/facebooki-konto-kaudu-saab-hinnata-laenaja-maksevoimet.d?id=66090580
46. Nicolaisen, N. (2010). *Getting StartED with Netbooks*. New York: Springer.
47. Nissenbaum, H. (1998). Protecting Privacy in an Information Age: The Problem of Privacy in Public. *Law and Philosophy*, 17, lk 559–596.
48. Nissenbaum, H. (2004). Privacy as Contextual Integrity. *Washington Law Review*, 79(30), lk 101–139.
49. Oolo, E.; Siibak, A. (2013). Performing for One's Imagined Audience: Social Steganography and Other Privacy Strategies of Estonian Teens on Networked Publics. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, 7 (1). URL: http://www.cyberpsychology.eu/view.php?cisloclanku=2013011501&article=7
50. Parksepp, A. (2014). Bigbank kasutab krediidianalüüsis Facebooki. *Majandus24.postimees.ee*, 12.august. URL: http://majandus24.postimees.ee/2885015/bigbank-kasutab-krediidianaluusis-facebooki
51. Post, R. (2001). Three Concepts of Privacy. *Georgetown Law Journal*, 89, lk 2087–2089.
52. Preston, J. (2011). Social Media Becomes a New Job Hurdle. *The New York Times*, 21. juuli. URL: http://www.nytimes.com/2011/07/21/technology/social-media-history-becomes-a-new-job-hurdle.html
53. Puuraid, P. (2012). Haiglaõde riputas intensiivravile sattunud sureva lapse pildi Facebooki. *Eesti Päevaleht*, 28. juuni. URL: http://epl.delfi.ee/news/eesti/haiglaode-riputas-intensiivravile-sattunud-sureva-lapse-pildi-facebooki.d?id=64603328
54. Rachels, J. (1975). Why Privacy is Important? *Philosophy and Public Affairs*, 4, lk 323–333.
55. Rebane. M. (2014). Google'it andmeid kustutama sundiva kohtuotsuse Eestis rakendamine võib olla keeruline. *ERR Uudised*, 18. mai. URL: http://uudised.err.ee/v/eesti/8f7b6216-e0a6-4a91-be87-5eb644f76953
56. Rosen, J. (2004). The Naked Crowd: Reclaiming Security and Freedom in an Anxious Age. *Workshop, Florida State University veebilehekülg*. URL: http://www.law.fsu.edu/faculty/2003-2004workshops/rosen.pdf
57. Rosen, J. (2010). The Web Means the End of Forgetting. *The New York Times*, 21. juuli. URL: http://www.nytimes.com/2010/07/25/magazine/25privacy-t2.html?_r=1
58. Roth, L. P.; Bobko, P.; van Iddekinge, C. H.; Thatcher, J. B. (2013). Social Media in Employee-Selection-Related Decisions: A Research Agenda for Uncharted Territory. *Journal of Management*, 20(10).
59. Runnel, P. (2010). Digitaalsest kirjaoskusest kodanikuaktiivsuseni. *Postimees*, 23. jaanuar. URL: http://arvamus.postimees.ee/215402/pille-runnel-digitaalsest-kirjaoskusest-kodanikuaktiivsuseni
60. Rössler, B. (2005). The Value of Privacy. Polity Press.
61. Schoeman, F. D. (1984). Privacy: Philosphical Dimensions of the Literature. Schoeman, F. D. (toim). *Philosophical Dimensions of Privacy: An Anthology*. Cambridge: Cambridge University Press, lk 1–34.
62. Sibicca, A. J.; Wesson, S. K. (2012). The Dermatologist and Social Media: The Challenges of Friending and Tweeting. Bercovitch, L.; C. Perlis (toim*). Contemporary*

Ethics and Professionalism in Dermatology Dermatoethics. London: Springer. Lk 77–83.
63. Siibak, A.; Murumaa, M. (2011). Exploring the 'Nothing to Hide' Paradox: Estonian Teens Experiences and Perceptions about Privacy Online*. Konverentsiartikkel. A Decade In Internet Time: OII Symposium on the Dynamics of the Internet and Society*, Oxford, 21.-24. september. URL: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1928498
64. Siibak, A.; Suder, S. (2013). Ülemus kui "suur vend". *Kommunikatsiooni- ja suhtekorralduse ajakiri Kaja*, 4, lk 13–14.
65. Slattery, J. (2010). S.I. Woman Allegedly Faked Jury Duty to Take Vacation. *CBS New York*, 28. oktoober. URL: http://newyork.cbslocal.com/2010/10/28/s-i-woman-allegedly-faked-jury-duty-to-take-vacation/
66. Solove, D. J. (2002). Conceptualizing Privacy. *California Law Review,* 90, lk 1087–1155. URL: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=313103
67. Solove, D. J. (2007). 'I've Got Nothing to Hide' and Other Misunderstandings of Privacy. *San Diego Law Review,* 44, lk 745-772. URL: http://ssrn.com/abstract=998565
68. Streitfeld, D. (2014). European Court Lets Users Erase Records on Web. *The New York Times*, 13. mai. URL: http://www.nytimes.com/2014/05/14/technology/google-should-erase-web-links-to-some-personal-data-europes-highest-court-says.html?_r=2
69. Šmutov, M. (2007). SEB Ühispanga töötajad mõnitasid räigelt kliente. *Postimees Online*, 8. veebruar. URL: http://e24.postimees.ee/1628091/seb-uhispanga-tootajad-monitasid-raigelt-kliente
70. Steeves, Valerie (2009). Reclaiming the Social Value of Privacy. Kerr, I., Steeves, V. and Lucock, C. (toim). *Privacy, Identity and Anonymity in a Network World: Lessons from the Identity Trail*. New York: Oxford University Press, 191–208.
71. Teder, M. (2012). Kohtud saavad õiguse Facebookis inimesega ühendust võtta. *Postimees*, 25. märts. URL: http://www.postimees.ee/783758/kohtud-saavad-oiguse-facebookis-inimesega-uhendust-votta
72. Tigas, K. (2013). Noored müüjad sõimavad Facebookis avalikult kliente! *Õhtuleht Online*, 6. november. URL: http://www.ohtuleht.ee/552584/noored-muujad-soimavad-facebookis-avalikult-kliente
73. Titiriga, R. (2011). Social Transparency through Recommendation Engines and Its Challenges: Looking Beyond Privacy. *Informatica Economica*, 15(4), lk 147-155. URL: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1944728
74. Umphress E. E.; Tihanyi, L.; Bierman, L.; Gogus, C.I. (2013). Personal Lives? The Effects of Nonwork Behaviors on Organizational Image. *Organizational Psychology Review*, 3(3), lk 199-221.
75. Visamaa, K. (2012). *Veebipõhiste sotsiaalvõrgustike kasutamine töötajate värbamisel*. Bakalaureusetöö, juh. A. Siibak, Tartu Ülikool, ajakirjanduse ja kommunikatsiooni instituut. URL: http://dspace.utlib.ee/dspace/handle/10062/28010
76. Voog, A. (2014). Internetipoodidest ostmine on Eestis seni arvatust populaarsem. *Eesti Päevaleht*, 7. märts. URL: http://kasulik.delfi.ee/news/uudised/internetipoodidest-ostmine-on-eestis-seni-arvatust-populaarsem.d?id=68188085
77. Walther, J. B.; Van Der Heide, B.; Kim, S. Y.; Westerman, D.; Tom Tong, S. (2008). The Role of Friends' Appearance and Behavior on Evaluations of Individuals on Facebook: Are We Known by the Company We Keep? *Human Communication Research*. URL: https://www.msu.edu/~jwalther/vita/pubs/facebook_hcr.pdf
78. Westin, A. (1967). *Privacy and Freedom*. New York: Atheneum.
79. Wigan, M. R.; Clarke, R. (2013). Big Data's Big Unintended Consequences. *Computer*, 46(6), lk 46–53.
80. Williams, B. (1973). Problems of the self. Cambridge: Cambridge University Press.
81. Youn, S. (2009). Determinants of Online Privacy Concern and Its Influence on Privacy Protection Behaviors Among Young Adolescents. *Journal of Consumer Affairs*, 43(3),

lk 389–418. URL: http://onlinelibrary.wiley.com/doi/10.1111/j.1745-6606.2009.01146.x/full
82. Euroopa Parlamendi 12. märtsi 2014. aasta seadusandlik resolutsioon ettepaneku kohta võtta vastu Euroopa Parlamendi ja nõukogu määrus üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta. (2014). *Euroopa Parlament*. URL: http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2014-0212&language=ET
83. E-äri ja e-kaubanduse kasutamine Eestis ja kasutamise laiendamise võimalused. (2013). *Riigikantselei*. URL: http://www.itl.ee/static/files/37.Lopparuanne_-_E-ari_ja_e-kaubandus_1_6_avalik_2013.pdf
84. Index Blasts EU Court Ruling on "Right to be Forgotten". (2014). Index on Censorship, 13. mai 2014. URL: http://www.indexoncensorship.org/2014/05/index-blasts-eu-court-ruling-right-forgotten/
85. Kaitseväe ohvitser sõimas Afganistanis hukkunud kaitseväelast (2012). *Delfi*, 13. august 2012. URL: http://www.delfi.ee/news/paevauudised/eesti/kaitsevae-ohvitser-soimas-afganistanis-hukkunud-kaitsevaelast.d?id=64813704
86. Kodanike rahulolu riigi poolt pakutavate avalike e-teenustega 2012. (2012). Majandus- ja Kommunikatsiooniministeeriumi tellitud TNS Emori uuring. URL: https://www.mkm.ee/sites/default/files/content-editors/failid/E_riik/uuring_kodanike_rahulolu_riigi_poolt_pakutavate_avalike_e-teenustega_2012_emor.pdf
87. Progress on EU data protection reform now irreversible following European Parliament vote. (12. märts 2014). *Europa.eu press releases database*. URL: http://europa.eu/rapid/press-release_MEMO-14-186_et.htm
88. Eurobaromeetri eriuuring 359: Attitudes on Data Protection and Electronic Identity in the European Union. (2011). *Euroopa Komisjon*. URL: http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf
89. Eurobaromeetri eriuuring 398: Internal market. (2013). *Euroopa Komisjon*. URL: http://ec.europa.eu/public_opinion/archives/ebs/ebs_398_en.pdf
90. Süsteemi turvalisus. (2014). *Eesti e-tervise sihtasutus*. URL: http://www.e-tervis.ee/index.php/et/uudised/uudiste-arhiiv/48-eestikeelsed-kategooriad/sihtasutus/tervise-infosysteem/251-systeemi-turvalisus
91. Tartu Ülikooli Eesti Geenivaramu. (2014). *Tartu Ülikooli Eesti Geenivaramu kodulehekülg*. URL: http://www.geenivaramu.ee/et/geenivaramust