TARTU ÜLIKOOL
ÕIGUSTEADUSKOND
Eraõiguse osakond

Anna Daniel

KÜPSISTE (*COOKIES*) JA MUUDE JÄLGIMISTEHNOLOOGIATE ANDMEKAITSEÕIGUSLIK REGULATSIOON EUROOPA LIIDU ÕIGUSES

Magistritöö

Juhendaja
Prof. Karin Sein

Tallinn
2021

Sisukord

Sissejuhatus

Elame ajastul, mil iga isiku igat liigutust võidakse potentsiaalselt varjatult jälgida ja jäädvustada, nagu logifailid salvestavad automaatselt arvutiprogrammi protsesse. Sellist praktikat on nimetatud ka elu logimiseks[1] ning sellist ühiskonnakorraldust jälgimiskapitalismiks, mis toitub iga üksikisiku igast inimkogemuse aspektist[2]. Jälgijaks ei ole sedapuhku mitte George Orwelli Suur Vend, sest isiku jälgimine avaliku sektori poolt on vähemalt demokraatlikes riikides küllalt rangelt reguleeritud, vaid jälgijaks on erasektor, kes on saanud alates interneti loomisest 1990. aastate algul peaaegu et takistamatult arendada välja üha uusi viise ja tehnoloogiaid aina suurema hulga andmete kogumiseks, töötlemiseks, teiste andmekogudega rikastamiseks ja kasumiga edasimüümiseks[3].

Üks tuntumaid ja levinumaid jälgimistehnoloogiaid on 1990. aastate keskpaigast pärit küpsised, mis on jätkuvalt aastas ülemaailmselt 300 miljardit dollarit maksva digireklaamitööstuse peamine hoob[4], kuid mille kõrvale on käitumispõhise reklaami esitamiseks kahekümne viie aasta jooksul arendatud arvukalt muid jälgimistehnoloogiaid. Nende tehnoloogiate abil saab mh tuvastada kasutajale tõenäoliselt kuuluvad seadmed, kasutaja seadme asukoha igal ajahetkel, külastatud veebisaidid ja neil viibitud aeg, nähtud reklaamid ja neile klõpsamised jpm[5]. Kogu see teave on suure väärtusega mitmesuguste reklaamitööstuse osapoolte jaoks, nagu reklaamivõrgustikud, andmevahendajad ja analüütikateenuste pakkujad, kes neid andmeid töötlevad ja kasutajaid profileerivad, et viia omavahel kokku veebisaidi omanikud, kes oma veebisaidil reklaamipinda välja üürivad ja sellega tulu teenivad, ning toodete ja teenuste pakkujad ehk reklaamijad, kes sel viisil läbimüüki suurendavad[6]. Seetõttu on andmeid nimetatud tänapäeva digiühiskonna valuutaks[7].

Reklaamitööstusele on küpsiste ja muude jälgimistehnoloogiate kasutamine peaaegu asendamatu teabeallikas, kuid üksikisiku jaoks tema eraelu puutumatust suure tõenäosusega

* Käesoleva töö valmimist on toetanud Eesti Teadusagentuuri grant PUT PRG 124.

[1] Mihaildis, A, Colonna, L. A Methodological Approach to Privacy by Design within the Context of Lifelogging Technologies. – Rutgers Computer and Technology Law Journal, Vol. 46, No. 1, 2020, lk 4–5.

[2] Zuboff, S. The Age of Surveillance Capitalism. The Fight for a Human Future at the New Frontier of Power. USA: Public Affairs, Hachette Book Group, 2019, lk 8–12.

[3] Judson, B. To understand where the cookie is headed, let's look at its history. Digital Content Next. (16.11.2020) – https://digitalcontentnext.org/blog/2020/11/16/to-understand-where-the-cookie-is-headed-lets-look-at-its-history/ (16.02.2021).

[4] Judson.

[5] Article 29 Data Protection Working Party. Working Document 02/2013 providing guidance on obtaining consent for cookies. 1676/13/EN, WP 208, 02.10.2013, lk 5–6; Digital Guide Ionos. What are cookies? (05.06.20) – https://www.ionos.com/digitalguide/hosting/technical-matters/what-are-cookies/ (17.04.2021).

[6] Zawadziński, M. What Is an Ad Network and How Does It Work? The Clearcode Blog. (20.20.2021) – https://clearcode.cc/blog/what-is-an-ad-network-and-how-does-it-work/ (22.02.2021).

[7] Council of Europe. European Commission for the Efficiency of Justice (CEPEJ). European Ethical Charter on the use of Artificial Intelligence in judicial systems and their environment. Adopted at the 31st plenary meeting of the CEPEJ. Strasbourg, 3–4 December 2018, lk 18.

tõsiselt riivav äripraktika. Küpsistega kogutavad andmed on enamasti isikuandmed isikuandmete kaitse üldmääruse (EL) 2016/679[8] (edaspidi IKÜM) tähenduses, sest sellise andmekogumise eesmärk reklaamitööstuses on teha järeldusi konkreetsete kasutajate huvide ja tõenäolise ostukäitumise kohta. Euroopa Liidu Kohus on mitmel korral tunnustanud elektroonilise side edastamise (ehk nt veebikasutuse) käigus tekkivate andmete konfidentsiaalsuse tähtsust eraelu puutumatuse kaitsel: „[n]eed andmed kokku võimaldavad teha väga täpseid järeldusi selliste isikute eraelu kohta, kelle andmeid säilitatakse, näiteks nende igapäevaelu harjumuste, alalise või ajutise elukoha, igapäevaste või muude liikumiste, tegevuste, sotsiaalsete suhete ja ühiskonnagruppide kohta, kellega nad läbi käivad."[9]

Reklaamitööstuse ja andmemajanduse kontrollimatu arengu tagajärjel on ülemaailmsest internetivõrgust – *world wide web* – kujunenud ülemaailmne metsik lääs – *world wide west*, märgiti juba 2009. aastal[10], mistõttu on initsiatiivi haaranud andmekaitse eestkõnelejad. Andmekaitse valdkonnas tuntud Max Schrems, kelle kaebuste alusel tunnistas Euroopa Liidu Kohus 2015. aastal kehtetuks USA-le isikuandmete edastamist võimaldava komisjoni otsuse USA andmekaitse piisava taseme kohta (Safe Harbour'i programm)[11] ning 2020. aastal sellele järgnenud sarnase komisjoni otsuse (Privacy Shield'i programm)[12], esitas 6. aprillil 2021. aastal Prantsusmaa andmekaitseasutusele kaebuse[13] Google'i vastu, sest Google'i toodetav operatsioonisüsteem Android määrab igale seadmele unikaalse identifikaatori nimega Android Advertising ID (AAID), millest kasutaja ei ole teadlik ega saa keelduda. AAID toimib mobiilseadmes, sh selle rakendustes samamoodi nagu küpsises salvestatav jälgimisidentifikaator (Tracking ID) veebikeskkonnas, võimaldades esitada seadme kasutajale käitumispõhist reklaami nii mobiilirakendustes kui ka veebis. See on vaid üks paljudest Schremsi algatatud menetlustest[14].

---

[8] 27. aprilli 2016. aasta Euroopa Parlamendi ja nõukogu määrus (EL) 2016/679 füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus). – ELT L 119, 04.05.2016, lk 1–88.

[9] Liidetud kohtuasjad EKo C-293/12 ja C-594/12, *Digital Rights Ireland Ltd* versus *Minister for Communications, Marine and Natural Resources jt* ning *Kärntner Landesregierung jt*, ECLI:EU:C:2014:238, p 26–27; Liidetud kohtuasjad EKo C-203/15 ja C-698/15, *Tele2 Sverige AB* versus *Post- och telestyrelsen* ning *Secretary of State for the Home Department* versus *Tom Watson jt*, ECLI:EU:C:2016:970, p 98–99.

[10] Kuneva, M. Roundtable on Online Data Collection, Targeting and Profiling. SPEECH/09/156. Brussels, 31.03.2009. – https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_09_156 (16.03.2021), lk 2–3.

[11] EKo C-362/14, *Maximillian Schrems* versus *Data Protection Commissioner*, ECLI:EU:C:2015:650.

[12] EKo C-311/18, *Data Protection Commissioner* versus *Facebook Ireland Ltd*, *Maximillian Schrems*, ECLI:EU:C:2020:559.

[13] Commission nationale de l'informatique et des libertés. Complaint under article 82 loi N° 78-17 du 6 janvier 1978. – https://noyb.eu/sites/default/files/2021-04/AAIDcomplaint_Redacted.pdf (27.04.2021).

[14] NOYB. 101 Complaints on EU-US transfers filed. (17.08.2020) – https://noyb.eu/en/101-complaints-eu-us-transfers-filed (27.04.2021).

Nende arengute taustal on Euroopa Liidu (edaspidi EL) seadusandja asunud üle vaatama 2002. aastast pärit ja 2009. aastal täiendatud e-privaatsuse direktiivi 2002/58/EÜ[15] (edaspidi ePD), mis reguleerib mh küpsiste ja muude jälgimistehnoloogiate kasutamist. 2017. aastal esitas komisjon ettepaneku[16] (edaspidi EK seisukoht) uue e-privaatsuse määruse (edaspidi ePM) vastuvõtmiseks, mille suhtes parlament kujundas oma seisukoha[17] (edaspidi EP seisukoht) sama aasta sügiseks. Pärast neli aastat kestnud vaidlusi jõudis nõukogu komisjoni esialgse ettepaneku suhtes viimaks ühise seisukohani[18] (edaspidi EN seisukoht) 2021. aasta veebruaris.

Käesolevas töös käsitletav õiguslik probleem on, kuidas tõsta uue ePM-i küpsiste ja muude jälgimistehnoloogiate regulatsiooniga EL-is eraelu puutumatuse kaitse taset, arvestades seejuures võimalust mööda reklaamitööstuse huvidega. Magistritöö eesmärk on pakkuda küpsiste ja muude jälgimistehnoloogiate reguleerimiseks välja lahendusi, mis tooksid kaasa muutuse, oleksid praktikas rakendatavad ning mille abil isikute eraelu puutumatus oleks kaitstud ja samas andmetöötlus, mis isikute õigusi ei riiva, saaks toimuda. Käesolevas töös püütakse leida vastused järgmistele uurimisküsimustele:

(1) Mis on küpsised ja muud jälgimistehnoloogiad ja millised on neist lähtuvad ohud eraelu puutumatusele seoses nende kasutusega reklaamitööstuses?
(2) Kuidas on küpsiste ja muude jälgimistehnoloogiate kasutamist EL-is siiani reguleeritud ning millistel tingimustel tohib kehtiva regulatsiooni kohaselt küpsiste ja muude jälgimistehnoloogiate abil koguda andmeid veebi ja nutiseadmete kasutajate kohta?
(3) Millised on peamised vaidlusküsimused menetletavas e-privaatsuse määruses küpsiste ja muude jälgimistehnoloogiate reguleerimisel ja millised oleksid neile sobivad lahendused?

Töös ei analüüsita küpsiste ja muude jälgimistehnoloogiate sellist kasutust, mis on vajalik kasutaja soovitud infoühiskonna teenuse osutamiseks, seadme turvalisuse tagamiseks, tarkvara uuenduste läbiviimiseks, õiguskaitse ja julgeoleku tagamiseks jms eesmärkidel, vaid töö

[15] 12. juuli 2002. aasta Euroopa Parlamendi ja nõukogu direktiiv 2002/58/EÜ, milles käsitletakse isikuandmete töötlemist ja eraelu puutumatuse kaitset elektroonilise side sektoris (eraelu puutumatust ja elektroonilist sidet käsitlev direktiiv). – EÜT L 201, lk 37–47 (eestikeelne eriväljaanne: ptk 13, kd 29, lk 514–524).
[16] Euroopa Komisjon. Ettepanek: Euroopa Parlamendi ja nõukogu määrus, milles käsitletakse eraelu austamist ja isikuandmete kaitset elektroonilise side puhul ning millega tunnistatakse kehtetuks direktiiv 2002/58/EÜ (privaatsust ja elektroonilist sidet käsitlev määrus). COM(2017) 10 final, 2017/0003 (COD). Brüssel, 10.01.2017.
[17] Euroopa Parlament. Raport ettepaneku kohta võtta vastu Euroopa Parlamendi ja nõukogu määrus, milles käsitletakse eraelu austamist ja isikuandmete kaitset elektroonilise side puhul ning millega tunnistatakse kehtetuks direktiiv 2002/58/EÜ (privaatsust ja elektroonilist sidet käsitlev määrus). (COM(2017)0010 – C8-0009/2017 – 2017/0003(COD)), A8-0324/2017, 20.10.2017.
[18] Council of the European Union. Mandate for negotiations with EP on Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications). Interinstitutional File: 2017/0003(COD). 6087/21. Brussels, 10.02.2021.

fookuses on küpsiste ja muude jälgimistehnoloogiate kaudu andmekogumine reklaamitööstuses ehk ärilistel eesmärkidel.

Töös kasutatakse dogmaatilist meetodit, sest autor analüüsib valdavalt kehtivat õigust, selle muutmiseks komisjoni, parlamendi ja nõukogu välja pakutud lahendusi ning eri lahenduste tähendust ühelt poolt andmesubjekti ja teiselt poolt reklaamitööstuse osapoolte jaoks.

Magistritöö esimeses peatükis küpsiste ja muude jälgimistehnoloogiate olemuse selgitamisel tugineb autor peamiselt veebiallikatele, kuivõrd tegemist on kiirelt areneva valdkonnaga, mille kõik võimalused ei pruugi raamatukaante vahele jõudagi. Veebiallikaid on kasutatud küpsiste ja reklaamitööstuse tehniliste aspektide kirjeldamiseks, mitte õigusliku analüüsi põhistamiseks. Töö teises ja kolmandas peatükis on allikatena kasutatud kehtivaid õigusakte, komisjoni, parlamendi ja nõukogu seisukohti, eri institutsioonide ettepanekuid, mõjuhinnanguid ja arvamusi, õiguskirjandust ning Euroopa Liidu Kohtu praktikat. Et juhtida tähelepanu teatud probleemide juurtele ja põhjendada nendes küsimustes otsustavate reformide vajadust, viitab autor ka vanematele allikatele 2000. aastatest.

Kodumaiseid allikaid on töös kasutatud minimaalselt, sest eestikeelseid õigusteaduslikke käsitlusi küpsiste ja muude jälgimistehnoloogiate kasutamise kohta reklaamitööstuses autorile teadaolevalt ei ole. Eestis on küll uuritud küpsiste turvalisust infotehnoloogilisest küljest[19], välismaa ülikoolides on mh analüüsitud küpsiste teavitusi ja nõusoleku küsimist[20] ning sarnaselt käesolevale tööle nõusoleku nõuet kasutaja tuvastamiseks internetis mitmesugustel eesmärkidel, sh käitumispõhise reklaami esitamiseks[21], kuid need uurimused ei käsitle uue ePM-i menetlemisel väljapakutud lahendusi ega saakski käsitleda alles 2021. aasta veebruaris avaldatud nõukogu ametlikku positsiooni. Seega on käesoleva töö panus Eesti õigusteadusesse küpsiste ja muude jälgimistehnoloogiate andmekaitseõigusliku regulatsiooni kaardistamine kehtiva õiguse järgi ja võimaliku tulevikus kehtima hakkava otsekohalduva regulatsiooni analüüs, mida on seostatud reklaamitööstuse huvidega.

Käesolevas magistritöös on kolm suuremat peatükki. Töö esimeses peatükis kirjeldatakse küpsiste ja muude jälgimistehnoloogiate olemust ja tööpõhimõtteid ning seostatakse neid reklaamitööstuses levinud ärimudelite ja neist lähtuvate andmekaitseõiguslike probleemidega. Teises peatükis kirjeldatakse küpsistele ja muudele jälgimistehnoloogiatele kohalduvat kehtivat õigust, sh analüüsitakse ePD seoseid isikuandmete kaitse üldmäärusega,

[19] Khandekar, C. Cookie Security and its Implementation in the Light of GD-PR and E-Privacy Regulation. Magistritöö. Tallinn University of Technology School of Information Technologies, 2019.
[20] From, A. Cookie Consents and Notices under the EU Data Protection Framework. Master's Thesis. University of Helsinki, 2020.
[21] Diemberger, C. Das datenschutzrechtliche Einwilligungserfordernis für den Einsatz von Identifikatoren zur Wiedererkennung von Internetnutzern im World Wide Web. Universität Wien, 2018.

üldmäärusest tulenevaid kehtiva nõusoleku tingimusi ning küpsiste kasutamise õiguslikke aluseid. Kolmas peatükk keskendub küpsiste ja muude jälgimistehnoloogiatega seotud sätete analüüsile komisjoni, parlamendi ja nõukogu seisukohtades, eeskätt küpsiste kasutamiseks nõusoleku andmise viisidele, nendega seotud probleemidele, eranditele nõusoleku nõudest ning uue ePM-i rakendamisele ja jõustamisele.

Märksõnad: andmekaitse, andmetöötlus, isikuandmed, privaatsus, e-turundus

1 Küpsiste (*cookies*) ja muude jälgimistehnoloogiate tähendus andmekaitseõiguses ja kasutus reklaamitööstuses

1.1 Küpsiste olemus ja neist lähtuv oht eraelu puutumatusele

Juba enam kui kümme aastat ehk alates e-privaatsuse direktiivi täiendamisest 2009. aastal on veebikasutajad pea igal sammul kokku puutunud küpsiste lubamise taotlustega mitmesugustel veebisaitidel, mis sageli võimaldavad kasutajal vaid küpsiste salvestamisega nõustuda. Kui küpsiste olemasolust on veebikasutaja enamasti teadlik, siis nende toimimispõhimõtetest sageli mitte. Kuid küpsised on olnud osa meie internetikogemusest märksa kauem kui eespool viidatud 2009. aasta, mil Euroopa Liidus võeti vastu nn *cookie law*, millega muudeti 2002. aastast pärit ePD-d.

Küpsise programmeeris 1994. aastal Lou Montulli, kes tegeles tol ajal ühega esimestest ja populaarsematest veebilehitsejatest Netscape Navigator. Montulli seisis silmitsi ühe kliendi probleemiga, kes soovis, et veebilehitseja jätaks meelde kasutaja valitud tooted kliendi veebisaidi[22] erinevatel veebilehtedel ning esitaks need üheskoos ostu sooritamise hetkel. Sisuliselt oli tegemist tänaseks tavalise, kuid tollal uudse virtuaalse ostukorviga. Klient ei soovinud hoida teavet pooleliolevate tehingute kohta enda serverites, vaid soovis leida võimaluse säilitada see teave iga kasutaja arvutis. Montulli ja tema meeskond programmeerisid väikese tekstifaili, mille veebilehitseja salvestas veebisaidi külastaja arvutisse ning mis jättis meelde külastaja tegevuse veebisaidil.[23] E-poe ostukorv on muide tänini üks peamine näide veebisaidi toimimiseks vajalikest küpsistest, mida käsitletakse allpool küpsise liikide juures[24].

Andmevahetus veebis rajaneb hüperteksti edastusprotokollil (HTTP ehk *HyperText Transfer Protocol*), mille abil toimib suhtlus veebilehitseja ja serveri vahel. Kasutaja esitab veebilehitseja kaudu päringu saada teavet (nt klõpsab lingil) ning server, kus soovitud veebilehte hoitakse, saadab veebilehitsejale vastusena soovitud veebisisu või võimaldab laadida alla soovitud faili. Pärast serverilt vastuse saamist katkestab veebilehitseja serveriga ühenduse,

---

[22] Sõnad „veebisait" ja „veebileht" ei ole samatähenduslikud. Veebisait on ühise veebiaadressi algusosaga veebilehekülgede kogum. Veebilehekülg ehk veebileht on veebis kindlat aadressi omav dokument, mis võib sisaldada teksti, pilte, helisid, programme või viiteid teistele lehekülgedele. Veebilehest võibki mõelda kui ühest A4 dokumendist, mida hoitakse veebiserveris ja kuvatakse kasutajale iga päringu korral. Veebileht on sisuliselt veebisaidi üks alamleht. Sarnaselt eristatakse sõnu *website* ja *webpage* inglise keeles. EKSS *sub vero* veebisait. – https://www.eki.ee/dict/ekss/index.cgi?Q=veebisait&F=M (16.02.2021); EKSS *sub vero* veebilehekülg. – https://www.eki.ee/dict/ekss/index.cgi?Q=veebilehek%C3%BClg&F=M (16.02.2021); Java T Point. Difference between Webpage and Website. (*sine anno*) – https://www.javatpoint.com/webpage-vs-website (16.02.2021); MDN Web Docs. Mozilla. What is the difference between webpage, website, web server, and search engine? (*sine anno*) – https://developer.mozilla.org/en-US/docs/Learn/Common_questions/Pages_sites_servers_and_search_engines (16.02.2021).

[23] Wikipedia *sub vero* HTTP cookie. – https://en.wikipedia.org/wiki/HTTP_cookie (16.02.2021); Judson.

[24] CookiePro. What are Strictly Necessary Cookies? (11.12.2020) – https://www.cookiepro.com/knowledge/what-are-strictly-necessary-cookies/ (16.02.2021).

mistõttu käsitleb server igat järgmist veebilehitseja päringut kui esmakordset ja eelnevatest sõltumatut. Veebiserver on näide olekuvabast ehk olekuta (*stateless*) serverist, mis võtab vastu päringuid, mis määravad täielikult ära soovitud dokumendi ega vaja mingit konteksti või eelmiste päringute meelespidamist. Olekuta serverile vastandub olekuga (*stateful*) server, mis võimaldab sellist ühendust, mis on võimeline protsessi või tehingu olekut säilitama protsessi või tehingu algusest lõpuni. HTTP on olemuslikult olekuta andmeedastusprotokoll, kuid oleku meeldejätmiseks lisatakse sellele küpsiseid.[25]

HTTP toimib pideva sõnumivahetusena veebilehitseja ja serveri vahel. Nii päring kui ka vastus koosneb kolmest osast:

1) Päringu (või vastuse) rida, mis on alati esimene;
2) Päringu (või vastuse) päis, milles sisalduvad protsessi, tehingut või ka sisu kirjeldavad metaandmed, nagu päringu kellaaeg, aktsepteeritav tähemärkide komplekt ja (inim)keel, kodeerimine, serveri ja veebilehitseja tehnilised andmed jms;
   (tühi rida)
3) Päringu (või vastuse) sisu, nt soovitud veebileht.[26]

Küpsis on väike tekstifail, mis lisatakse päringule vastamise käigus vastuse päisesse teiste metaandmete kõrvale ning salvestatakse kasutaja arvuti kõvakettale. Iga kord, kui kasutaja liigub veebilehitsejas uuesti samale veebisaidile, saadab veebilehitseja vastavale serverile ka küpsise. Kui server saab veebilehitsejalt küpsist sisaldava päringu, kasutab server küpsisesse salvestatud andmeid ja saadab nende alusel veebilehitsejale just kasutajale sobiva veebisisu.[27]
Küpsise seadmine näeb lihtsustatult välja järgmine:

1) Päring: kasutaja külastab veebisaidi *www.example.org* alamlehte *index.html*. Veebilehitseja saadab soovitud veebisaidi serverile päringu alamlehe kuvamiseks:

```
GET /index.html HTTP/1.1
Host: www.example.org
User-Agent: Mozilla/4.0 (MSIE 6.0; Windows NT 5.1)
...
```

2) Vastus: soovitud veebisaidi server saadab veebilehitsejale teabe alamlehe kuvamiseks ning lisab vastuse päisesse kaks küpsist:

```
HTTP/1.0 200 OK
User-Agent: Mozilla/4.0 (MSIE 6.0; Windows NT 5.1)
```

[25] Wikipedia *sub vero* Hypertext Transfer Protocol. – https://en.wikipedia.org/wiki/Hypertext_Transfer_Protocol (16.02.2021); Wikipedia *sub vero* World Wide Web. – https://en.wikipedia.org/wiki/World_Wide_Web (16.02.2021); Wikipedia *sub vero* Web server. – https://en.wikipedia.org/wiki/Web_server (16.02.2021); E-teatmik *sub vero* HTTP (HyperText Transfer Protocol), WWW (World Wide Web), state, stateful, stateless, URL (Uniform Resource Locator). – http://vallaste.ee/ (16.02.2021); Kristol, D. M. HTTP Cookies: Standards, Privacy, and Politics. – ACM Transactions on Internet Technology, Vol. 1, No. 2, November 2001, lk 152.
[26] Kristol, lk 152–153; E-teatmik *sub vero* HTTP header, cookie, third party cookie. – http://vallaste.ee/ (16.02.2021); Wikipedia *sub vero* HTTP cookie.
[27] Kristol, lk 152–153; E-teatmik *sub vero* HTTP header, cookie, third party cookie. – http://vallaste.ee/ (16.02.2021); Wikipedia *sub vero* HTTP cookie.

```
Content-type: text/html
Set-Cookie: theme=light
Set-Cookie: sessionToken=abc123; Expires=Wed, 09 Jun 2021
10:18:14 GMT
...
```

3) Uus päring: kasutaja külastab sama veebisaidi *www.example.org* teist alamlehte *spec.html*. Veebilehitseja saadab soovitud veebisaidi serverile päringu alamlehe kuvamiseks ja lisab päringule eelneva külastuse käigus seatud küpsised:

```
GET /spec.html HTTP/1.1
Host: www.example.org
User-Agent: Mozilla/4.0 (MSIE 6.0; Windows NT 5.1)
Cookie: theme=light; sessionToken=abc123
...
```

Tänu küpsistele oskab veebisaidi server siduda uue külastuse varasemaga. Uuele päringule vastamise käigus võidakse küpsiseid muuta, lisada või kustutada.[28]

Lisaks eespool mainitud e-poe ostukorvi sisule võivad küpsised salvestada teavet sisselogimise, registreerimise, tarneinfo (nt nimi, postiaadress), arvete, maksevahendite, valuuta ja kasutajavalikute kohta veebisaidil, kuid ka kasutaja veebitegevust, sh klõpsatud linke ja varem külastatud veebisaite. Paljud küpsised täidavad veebi ja mitmesuguste teenuste toimimiseks vajalikke funktsioone. Nt autentimisküpsised on vajalikud, et veebiserver teaks, kas ja millise konto all kasutaja on mõnda teenusesse või veebikeskkonda sisse loginud. Kasutaja navigeerib sageli veebisaidi alamlehtedel mitu korda edasi-tagasi. Nt avab kasutaja e-kirja ja liigub pärast selle lugemist tagasi e-postkasti, seejärel avab uue e-kirja. Internetipangas võib kasutaja soovida vaadata e-arveid, seejärel konto väljavõtet ja investeeringute seisu, mis kõik asuvad eraldi internetipanga veebilehtedel. Ilma sellise mehhanismita ei teaks server järgmise veebilehe kuvamisel, kas saata veebilehitsejale tundlikku teavet sisaldavat veebisisu või nõuda kasutajalt sisselogimise teel enda tuvastamist. Ilma autentimisküpsisteta peaks kasutaja oma e-postkastis iga kord, kui ta vajutab veebilehitsejas „Tagasi" nuppu, uuesti oma parooli sisestama.[29]

Küpsiseid võib liigitada päritolu alusel esimese ja kolmanda osapoole küpsisteks (*first-party vs third-party*) ning kestuse alusel sessiooni- ja püsiküpsisteks (*session vs permanent cookies*). Esimese osapoole ehk autoriküpsised salvestab kasutaja arvutisse külastatav veebisait ise, kolmanda osapoole ehk võõrküpsised kuuluvad mõnele muule

[28] Wikipedia *sub vero* HTTP cookie; Vikipeedia, *sub vero* HTTP-küpsis. – https://et.wikipedia.org/wiki/HTTP-k%C3%BCpsis (17.02.2021).
[29] Kristol, lk 152–153; E-teatmik *sub vero* cookie. – http://vallaste.ee/ (17.02.2021); Wikipedia *sub vero* HTTP cookie.

veebisaidile[30], kes salvestab need kasutaja arvutisse enamasti analüütika ja turunduse eesmärgil. Sessioonikküpsiseid kasutatakse vaid veebisaidi külastamise ajal ning need kustutatakse veebilehitseja sulgemisel (eespool toodud näites `Set-Cookie: theme=light`, sest küpsise tähtaja kohta teave puudub). Püsiküpsiseid kasutatakse informatsiooni salvestamiseks pikema aja vältel (nt selleks, et hoida kasutajat teenusesse sisselogituna) ning need kustutatakse kas kindlaksmääratud tähtpäeval või tähtaja möödumisel (eespool toodud näites `Set-Cookie: sessionToken=abc123`, sest küpsise kustumistähtpäevaks on määratud 9. juuni 2021). Püsiküpsise eluea jooksul saadetakse küpsis vastavale veebisaidile tagasi iga kord, kui kasutaja külastab küpsise seadnud veebisaiti või mõnda selle partnerveebisaiti. Nt on paljud veebisaidid omavahel seotud ühise partneri – reklaamivõrgustiku – kaudu. Seetõttu nimetatakse püsiküpsiseid ka jälgimisküpsisteks (*tracking cookies*), sest need võimaldavad jälgida kasutaja veebitegevust pika aja jooksul ja veebisaitideüleselt.[31] Tehnoloogia teemalistes foorumites uuriti juba kümne aasta eest, kas on võimalik programmeerida igavesti kestev küpsis, ning anti nõu, kuidas saavutada paremuselt järgmine lahendus: valida kuupäev, mis on väga kauges tulevikus[32]. Nõnda praktikas tehaksegi. Artikli 29 andmekaitse töörühma 2015. aasta uurimus näitas, et kuigi enamasti on küpsise kestus paar aastat, esineb küpsiseid, mille kustumistähtaeg on 31/12/9999 23:59, millest nähtub suurim lubatud väärtus neljakohalisel aasta väljal[33].

Lisaks päritolule ja kestusele võib küpsiseid liigitada eesmärgi alusel. Üks võimalik liigitus on järgmine, kusjuures küpsis võib kuuluda korraga mitmesse kategooriasse:

1) Vajalikud küpsised (*necessary cookies*) on hädavajalikud veebisaidi toimimiseks ja selle funktsioonide kasutamiseks. Vajalikud küpsised võimaldavad kasutajal kasutada teenuseid, milleks ta on konkreetselt soovi avaldanud, nt vaadata videot[34] või pääseda

[30] Veebisaitide kontekstis eristatakse esimese ja kolmanda osapoole küpsiseid domeeninime järgi. Domeeninimi on nähtav veebilehitseja aadressiribal ning ühe veebisaidi kõigil alamlehtedel on sama domeeninimi. Infotehnoloogias peetakse kolmanda osapoole küpsiste all silmas küpsiseid, mida salvestavad muu domeeninimega veebisaidid kui see veebisait, mida kasutaja külastab. Article 29 Data Protection Working Party. Opinion 04/2012 on Cookie Consent Exemption. 00879/12/EN, WP 194, 07.06.2012, lk 4.

[31] Cookiebot. Cookie checker. Is your website GDPR and CCPA compliant? (01.04.2020) – https://www.cookiebot.com/en/cookie-checker/ (11.02.2021); Wikipedia *sub vero* HTTP cookie; Tartu Ülikool, arvutiteaduse instituut. Õppeaine Infoturve (MTAT.07.028). Privaatsus ja anonüümsus veebis – https://courses.cs.ut.ee/2018/infsec/spring/Main/Loeng-Anon%C3%BC%C3%BCmsusVeebis (17.02.2021).

[32] Stack Overflow. Set a cookie to never expire. (*ca* 2010) – https://stackoverflow.com/questions/3290424/set-a-cookie-to-never-expire (20.02.2021).

[33] Article 29 Data Protection Working Party. Cookie Sweep Combined Analysis – Report. 14/EN, WP 229, 03.02.2015, lk 19.

[34] Küpsised on video vaatamiseks vajalikud, kui video vaatamine ongi teenuse sisuks (nt Youtube'i saidil videote vaatamine), kuid neid küpsiseid ei või kasutada muul otstarbel, nagu veebianalüütika või teenuse personaliseerimine. Information Commissioner's Office (ICO). Guidance on the use of cookies and similar technologies. Version 1.0.48. UK: ICO, 2019, lk 36.

ligi enda tuvastamist nõudvale veebisisule. Tavaliselt on tegemist esimese osapoole sessiooniküpsistega;

2) Analüütika- ehk statistikaküpsised (*analytics or statistics cookies*) (vahel ka toimivusküpsised, *performance cookies*) koguvad teavet selle kohta, kuidas kasutaja veebisaidil navigeerib, et parendada kasutuskogemust. Analüütikaküpsised ei ole vajalikud küpsised, sest kasutaja saab veebisaiti külastada ja nt uudiseid lugeda ka siis, kui analüütikaküpsised ei ole n-ö sisse lülitatud[35]. Analüütikaküpsised võimaldavad veebisaidil hinnata, milliseid veebilehti külastatakse kõige rohkem ning need kasutajale kättesaadavamaks teha, samuti tuvastada veebilehed, mis saadavad veateateid. Analüütikaküpsistega mõõdetakse reklaamlinkidele klõpsamiste arvu (nt *pay-per-click* ehk klikipõhise tasuarvestuse korral), kuid ei pruugita kasutajat identifitseerida. Analüütikaküpsistega kogutakse teavet enamasti anonüümselt ja agregeeritud kujul, kuid kui sama teavet kasutatakse hiljem samale isikule reklaami suunamiseks, on tegemist turundusküpsistega. Analüütikaküpsiste abil mõõdetakse ka ühelt veebisaidilt teisele suunamiste arvu ja sellele järgnenud kasutaja käitumist (nt sooritatud oste) ning arvestatakse suunajale komisjonitasu (*affiliate tracking*). Analüütikaküpsised võivad olla esimese või kolmanda osapoole küpsised, nt Google Analytics[36], Facebook Analytics[37] ja Adobe[38] pakuvad veebisaitidele analüüsiteenuseid, kuid veebisaidi omanik võib ka ise oma veebisaidi külastajate arvu mõõta;
3) Eelistuste ja funktsionaalsed küpsised (*preference and functionality cookies*) jätavad meelde kasutaja eelistused veebisaidil, nagu keel ja tekstisuurus, regioon ja valuuta (e-poes). Funktsionaalsete küpsiste abil kogutud teabe võib hiljem anonüümida ja need ei jälgi kasutaja veebikasutust muudel veebisaitidel. Kui seda siiski tehakse, on tegemist turundusküpsistega;
4) Turundus- ehk reklaamküpsised (*marketing or advertising cookies*) koguvad teavet kasutaja veebikäitumise ja -harjumuste kohta eesmärgiga pakkuda kasutajale tema huvidest lähtuvat reklaami. Nende abil tagatakse mh, et kasutaja ei näeks iga kord samu reklaame, ja mõõdetakse reklaamikampaaniate edukust. Turundusküpsised võivad olla nii esimese kui ka kolmanda osapoole küpsised, nt uudisteportaal võib reklaamida nii oma teenuseid kui ka muude ettevõtjate teenuseid ja tooteid. Teenuseid müüa soovivate ettevõtjate (*advertisers*) huvides võivad turundusküpsiseid kasutaja arvutisse salvestada ka reklaamivõrgustikud (*advertising network*). Reklaamivõrgustikud ja

[35] Information Commissioner's Office (ICO). Guidance on the use of cookies and similar technologies, lk 39.
[36] Google Marketing Platform. Analytics. – https://marketingplatform.google.com/about/analytics/ (17.02.2021).
[37] Facebook Analytics. – https://analytics.facebook.com/ (17.02.2021).
[38] Adobe Analytics. – https://www.adobe.com/analytics/adobe-analytics.html# (17.02.2021).

andmevahendajad (*data brokers*) salvestavad turundusküpsiste abil kasutaja tegevuse veebisaidil, seostavad selle teabe muudest allikatest pärit teabega, koostavad kasutaja profiili, ning müüvad seda teavet teistele isikutele.[39] Hinnanguliselt 99% küpsistest kasutatakse veebikäitumise jälgimiseks ja sihitud reklaami esitamiseks[40].

Kuigi veebikasutajad võivad olla personaalsetest pakkumisest huvitatud, võib enda kohta loodud profiili teadasaamine olla kõhedakstegev. Ühes ajakirjanduslikus uurimuses tuvastati näiteks, et küpsis koodiga 4c812db292272995e5416a323e79bd37 tähistab 26-aastast naist Nashville'ist Tennessee osariigis, kelle lemmikfilmide ja -seriaalide seas on „The Princess Bride", „50 First Dates", „10 Things I Hate About You" ja „Sex and the City" ning kellele meeldib lugeda kõmu-uudiseid ja lahendada *online*-viktoriine. See konkreetne andmesubjekt pidas enda kohta loodud profiili võõrastavalt täpseks. Ent reklaamivõrgustikud kategoriseerivad inimesi ka väga tundlike ja sügavalt isiklike tunnuste põhjal. Nt Yahoo suudab nimeliselt tuvastada äsja kooli lõpetanud neiu, kes on huvitatud kaalu langetamisest. Üks 32-aastane naine otsis teatud perioodil veebist teavet reproduktiivtervisega seotud probleemide kohta ning kuigi hiljem selgus, et tal neid terviseprobleeme ei ole, kuvatati talle endiselt mh viljatuse teemalisi reklaame.[41]

Tavaliste küpsiste kõrval on välja töötatud ka muid küpsiseid, nt Flash-küpsised (nim ka *local shared objects*) ja Trooja hobuse laadi küpsised (*Trojan horse cookies*). Flash-küpsiseid eristab tavalistest küpsistest see, et Flash-küpsised salvestatakse veebilehitseja küpsistest eraldi, mis tähendab, et need võimaldavad jälgida kasutaja tegevust veebilehitsejate-üleselt, ning et need tuleb kustutada tavaküpsistest eraldi. Tähelepanuväärsem on aga see, et Flash-küpsised suudavad taasluua tavalisi HTTP-küpsiseid, mille kasutaja on kustutanud, eirates nõnda kasutaja selgelt väljendatud tahet.[42] Trooja hobuse küpsised või üksteise sisse peidetud kihilised küpsised (*embedded cookies*) lubavad n-ö tagaukse kaudu veebisaidile veel hulga küpsiseid (nim ka neljanda osapoole küpsisteks), mille olemasolust

---

[39] International Chamber of Commerce UK (ICC). Cookie guide Second ed. November 2012. – https://www.cookielaw.org/wp-content/uploads/2019/12/icc_uk_cookiesguide_revnov.pdf (11.02.2021), lk 7–10; Cookiebot. GDPR and cookie consent. Compliant cookie use. (27.10.2020) – https://www.cookiebot.com/en/GDPR-cookies/ (17.02.2021).

[40] Urban, T., Degeling, M., Holz, T., Pohlmann, N. Beyond the Front Page: Measuring Third Party Dynamics in the Field. – WWW '20: Proceedings of The Web Conference 2020, alajaotis 5.1.

[41] Angwin, J. The Web's New Gold Mine: Your Secrets. (30.07.2010) – The Wall Street Journal. https://news.tfionline.com/post/888296348/the-webs-new-gold-mine-your-secrets/amp; https://www.wsj.com/articles/SB10001424052748703940904575395073512989404 (16.02.2021).

[42] González Guerrero, L. D. Control of Our Personal Data in the Big Data Era: The Case of Third Party Web Tracking. – Estudios Socio-Juridicos, Vol. 21, No. 1, January–June 2019, lk 217; Hoofnagle, C. J., Soltani, A., Good, N., Wambach, D. J., Ayenson, M. D. Behavioral Advertising: The Offer You Cannot Refuse. – Harvard Law & Policy Review, Vol. 6, Issue 2, 2012, lk 277–278; CookiePro. What is a Flash Cookie? (02.06.2020) – https://www.cookiepro.com/knowledge/what-is-a-flash-cookie/ (18.02.2021).

veebisaidi operaator rääkimata kasutajast ei ole teadlik[43]. Peale küpsiste kasutatakse veel jälgimispiksleid (*tracking pixels*), mis on läbipaistvad 1×1 piksli suurused pildifailid veebilehel, mis veebilehe laadimisel koguvad teavet kasutaja seadme ja veebilehitseja kohta, või e-kirja sisus, võimaldades jälgida, millal ja kui sageli kasutaja e-kirja avab.[44] Kuna jälgimispikslid on läbipaistvad, on tavakasutajal neid ilma eriteadmisteta võimatu tuvastada.

Kuigi paljud küpsised on veebi toimimiseks meile harjumuspärasel viisil vajalikud, ilmneb siiski ülaltoodud kirjeldustest ja arvukatest uurimustest, et küpsised ja muud jälgimistehnoloogiad võivad endast kujutada tõsist ohtu eraelu puutumatusele ja isikuandmete kaitsele. Märkimisväärne on asjaolu, et küpsise loomisega samaaegselt teadvustati ka sellega seotud privaatsusriske. David M. Kristol, kes koos küpsise looja Lou Montulliga töötas välja esimesed küpsiste tehnilised standardid RFC 2109[45] ja RFC 2965[46], mis avaldati vastavalt aastatel 1997 ja 2000, kirjeldas juba 2001. aastal ohte, mis lähtuvad kolmanda osapoole küpsistest, mis laetakse ühe veebisaidi külastamisel teise veebisaidi poolt kasutaja arvutisse ja millest kasutaja pole teadlik. Juba 1990. aastate lõpuks olid tekkinud reklaamivõrgustikud ja ärimudelid, mis rajanesid suunatud reklaami pakkumisel kolmanda osapoole küpsiste abil. Veelgi enam, juba siis oli selge, et kolmanda osapoole küpsised võimaldavad reklaamivõrgustikel luua profiile ja neid teiste ettevõtjatega jagada või neile müüa.[47] Varjatud ja automatiseeritud isikuandmete töötlemist internetis ning anonüümsuse kadumist taunis ka artikli 29 andmekaitse töörühm oma 1997. ja 1999. aastal välja antud suunistes[48].

Kasutajate profileerimine ja nende põhjal otsuste langetamine oli ja on tänini üheks keskseks probleemiks küpsiste ja muude jälgimistehnoloogiatega kogutud andmete töötlemisel[49]. Arvutusvõimsuse ja andmehulkade jätkuva kasvuga kaasneb võimalus luua üha täpsemaid profiile ja prognoose ning saada aina detailsem sissevaade üksikisiku eraellu[50]. Paljud kategooriad, millesse kasutajaid jaotatakse, on üsna ootuspärased ja mõistetavad, nt üliõpilased, auto-, kodu- või koeraomanikud või golfisõbrad. Kuid paljud kategooriad on

---

[43] European Digital Rights (EDRi) and Cookiebot. Ad Tech Surveillance on the Public Sector Web. A special report on pervasive tracking of EU citizens on government and health service websites. *Sine loco*, 2019, lk 4; Urban jt, alajaotis 4.5.

[44] CookiePro. Website Tracking Technologies. (28.10.2020) – https://www.cookiepro.com/knowledge/website-tracking-technologies/ (12.02.2021); E-teatmik *sub vero* web beacon. – http://vallaste.ee/ (16.02.2021).

[45] IETF (Internet Engineering Task Force). HTTP State Management Mechanism. RFC 2109. February 1997. – https://tools.ietf.org/html/rfc2109 (16.02.2021).

[46] IETF (Internet Engineering Task Force). HTTP State Management Mechanism. RFC 2965. October 2000. – https://tools.ietf.org/html/rfc2965 (16.02.2021).

[47] Kristol, lk 159–160, 163, 180.

[48] Article 29 Data Protection Working Party. Recommendation 1/99 on Invisible and Automatic Processing of Personal Data on the Internet Performed by Software and Hardware. 5093/98/EN/final, WP 17, 23.02.1999; Article 29 Data Protection Working Party. Recommendation 3/97 Anonymity on the Internet. XV D /5022/97 final, WP 6, 03.12.1997.

[49] Kristol, lk 163–164.

[50] OECD. Artificial Intelligence in Society. Paris: OECD Publishing, 2019, lk 58, 87; Popper, J. jt. Artificial intelligence across industries. White Paper. Geneva: International Electrotechnical Commission, 2018, lk 28.

kasutajate jaoks ootamatud ja diskrimineerivad, nt kategoriseerimine sissetuleku (tagasihoidliku sissetulekuga, kiirlaenu taotlejad, säästurežiimil pensionärid), päritolu (afroameeriklastest kiirlaenu taotlejad) ja tervise (diabeedihuvi, kolesterooli probleemid) alusel. Need on näited andmevahendajate endi sõnastatud kategooriatest, kuid turundajad otsivad sageli väga spetsiifilisi sihtrühmi, nagu teatud poliitiliste või usuliste vaadetega isikud või peagi pärima õigustatud isikud.[51]

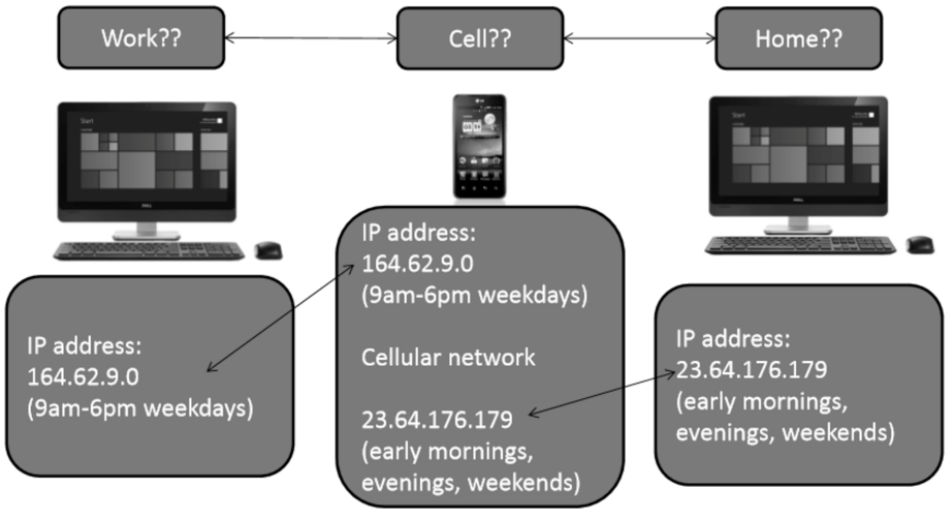
1.2 Muud jälgimistehnoloogiad ja nendest lähtuv oht eraelu puutumatusele

Küpsised pole kaugeltki ainus tehnoloogia, mille kaudu üksikisikute kohta andmeid kogutakse. Üks peamisi kriitika põhjuseid käesoleva töö kirjutamise ajal kehtiva e-privaatsuse direktiivi aadressil puudutab selle tehnoloogilist mahajäämust ehk mittearvestamist paljude uute tehnoloogiatega, mis sarnaselt küpsistele võimaldavad isikute jälgimist, kusjuures mitte üksnes virtuaalmaailmas (*online*), vaid ka nt ostukeskuses ja kodus (*offline*)[52].

Eri tehnoloogiate abil saab luua seadme „sõrmejälje" (*device fingerprinting*), mis salvestab seadme või tarkvaraga seotud tehnilisi andmeid, nagu operatsioonisüsteem ja selle seaded, veebilehitseja versioon, regioon, ajavöönd, IP-aadress, aku olek jpm. Seadme „sõrmejälje" loomist on keeruline kehtiva õiguse alusel takistada, sest kasutaja seadmesse ei salvestata midagi, vaid kogutakse andmeid seadme parameetrite kohta[53]. Eraldivõetuna ei ole need omadused seadme tuvastamiseks piisavad, kuid kombineerituna võimaldavad 100 000 veebilehitseja seast üheselt tuvastada 80–90% arvutitest ja 81% mobiiliseadmetest. Enamik kolmandaid osapooli kaupleb sedalaadi isikut tuvastavate identifikaatoritega ja müüb neid soovijatele.[54] Levinud on ka seadmeteülene jälgimine (*cross-device tracking*). Kui üks mobiiliseade kasutab tööpäevadel tööajal sama IP-aadressi ühe arvutiga, kuid õhtuti ja nädalavahetustel sama IP-aadressi teise arvutiga, siis võib sellest järeldada, et kõiki kolme seadet kasutab sama isik ning et esimene arvuti asub ilmselt isiku töökohas ja teine tema kodus[55]. Seda olukorda illustreerib Joonis 1.

[51] Vladeck, D. C. Consumer Protection in an Era of Big Data Analytics. – Ohio Northern University Law Review, Vol. 42, No. 2, 2016, lk 500.
[52] European Data Protection Supervisor. Opinion 5/2016. Preliminary EDPS Opinion on the review of the ePrivacy Directive (2002/58/EC). 22.07.2016, lk 3.
[53] Hoofnagle jt, lk 285.
[54] Englehardt, S., Narayanan A. Online Tracking: A 1-million-site Measurement and Analysis. – Computer Science Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security 2016, alajaotis 5.6 ja 6.
[55] Brookman, J., Rouge, P., Alva, A., Yeung, C. Cross-Device Tracking: Measurement and Disclosures. – Proceedings on Privacy Enhancing Technologies 2017(2), lk 135.

Joonis 1. Seadmeteülene jälgimine IP-aadressi abil

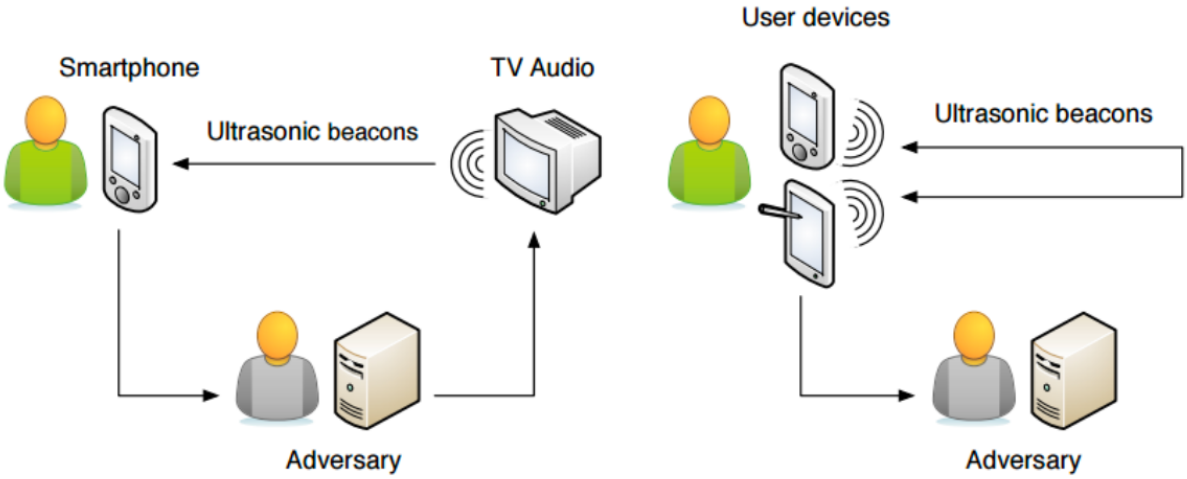


Allikas 1: Brookman jt, lk 135.

Asukoha ja isikuga seotud seadmete jälgimiseks kasutatakse ka ultrahelisignaale, mida üks seade edastab ning teiste seadmete mikrofonid vastu võtavad, aga mida inimkõrv ei kuule. Ühe Saksa ülikooli teadlased uurisid ultrahelisignaalide kasutust isikute jälgimisel. Joonis 2 kujutab vasakul olukorda, kus kõlaritega varustatud seade (nt televiisor, raadio) edastab nn ultrahelimajaka (*ultrasound beacon*) kaudu ultrahelisignaali ning mikrofoniga varustatud seade võtab helisignaali vastu. See võimaldab reklaamivõrgustikul koguda teavet isiku meediatarbimise kohta, nt millal, kui kaua, millise sisuga saateid isik vaatab. Teiste seas uurisid saksa teadlased Daniel Arp jt Silverpushi[56], üht esimestest ultrahelisignaali kasutavatest jälgimise rakendustest, mis oli 2017. aasta jaanuaris olemas juba 234 Androidi mobiilirakenduses, kuigi ultrahelisignaale edastavaid telereklaame saksa teadlased tol hetkel veel ei tuvastanud. Joonise paremal poolel illustreeritakse seda, kuidas seadmed omavahel ultrahelisignaali kaudu „suhtlevad", mis võimaldab tuvastada ühele isikule tõenäoliselt kuuluvaid seadmeid või omavahel sagedasti suhtlevaid isikuid ehk kasutaja tutvusringkonda. *Adversary* tähendab inglise keeles otsetõlkes „vaenlast", kuid tähistab nende jooniste kontekstis kolmandast osapoolest andmekogujat.

[56] SilverPushi globaalse haardega klientide nimekiri on muljetavaldav. SilverPush. – https://www.silverpush.co/ (17.02.2021).

Joonis 2. Kasutaja poolt tarbitava meedia ja tema poolt kasutatavate seadmete jälgimine ultrahelisignaalide abil

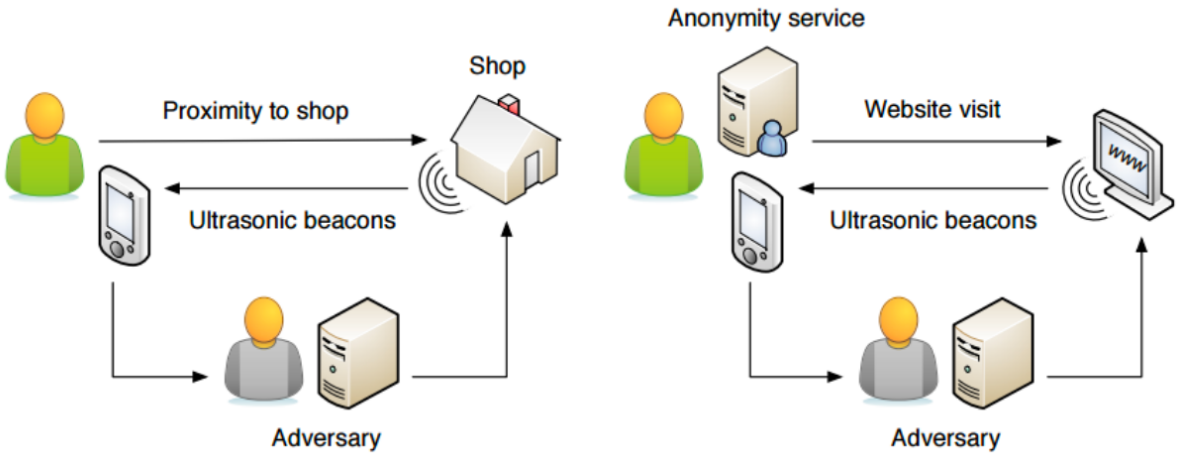


Allikas: Arp, D., Quiring, E., Wressnegger, C., Rieck, K. Privacy Threats through Ultrasonic Side Channels on Mobile Devices. – 2nd IEEE European Symposium on Security and Privacy. Paris: IEEE, 2017, lk 36.

Joonis 3 näitlikustab isiku füüsilise asukoha jälgimist ja andmete de-anonüümimist. Kaupluse sissepääsu juurde võib olla paigaldatud ultrahelimajakas, mis saadab ultrahelisignaali isiku mobiilseadmesse ning võimaldab teha järeldusi isiku asukoha ja huvide kohta. Kui isik külastab ostukeskuses mõnda brändipoodi ja tema külastus registreeritakse ultrahelisignaali abil, võidakse talle hiljem reklaamida vastava brändi tooteid ka juhul, kui isik pole kordagi selle brändi veebisaiti külastanud ega seda otsingumootori kaudu otsinud[57]. Joonise paremal poolel on näha, kuidas veebikäitumine on tuvastatav isegi kasutaja puhul, kes on võtnud meetmeid oma privaatsuse kaitsmiseks (nt keelanud ja kustutanud küpsised, aktiveerinud Do Not Track'i või AdBlock'i funktsiooni), kui veebisaidile on sisse kodeeritud ultrahelisignaal, mille kasutaja mobiilseade vastu võtab. Ultrahelisignaal ei sõltu WiFi vms ühenduse olemasolust, mis tähendab üsna avaraid kasutusvõimalusi ka väljaspool internetiühendust[58].

[57] Cookiebot. How do websites track users? Technologies and methods. GDPR Compliance. (*sine anno*) – https://cookiebot.dev/en/website-tracking/ (12.02.2021).
[58] O'Driscoll, A. How ultrasonic tracking apps may be listening to you and how to block them. (18.10.2019) – https://www.comparitech.com/blog/information-security/block-ultrasonic-tracking-apps/ (17.02.2021).

Joonis 3. Kasutaja asukoha jälgmine ja veebikäitumise de-anonüümimine ultrahelisignaalide abil



Allikas: Arp, lk 36.

Seadmetevahelisele suhtlusele mitmesuguste sensorite abil rajaneb ka asjade internet (*Internet of Things*): nutiseadmed, tervisemonitorid, arukad autod ja kodumasinad võivad koguda, salvestada, töödelda ja edastada pidevalt ja varjatult andmeid isikute tervise, käitumise, harjumuste ja neid ümbritseva keskkonna kohta. Google avaldas 2013. aastal Ameerika Ühendriikide Väärtpaberite ja Börsitehingute Komisjonile, et vaid mõne aasta pärast võib osutuda võimalikuks esitada reklaame ja muud sisu mh külmkapil, auto armatuurlaual, termostaadil ja käekellal.[59] Kuigi asjade interneti tehnoloogiaid võidakse kasutada ka muudes valdkondades (nt tööstuses, meditsiinis[60]), töödeldakse selle tehnoloogia varjus sageli konkreetset füüsilist isikut tuvastada võimaldavaid andmeid, mistõttu on asjade internetti tabavalt nimetatud mitte lihtsalt „asjade internetiks", vaid „inimestega seotud asjade internetiks".[61]

Paljud suurkorporatsioonid, nagu Microsoft, Apple ja Google jälgivad isikute asukohta nii seadmete kui ka konto seadete kaudu, mis on vaikimisi seadistatud asukohaandmeid jagama (vt ka juhiseid asukohaandmete jagamise väljalülitamiseks)[62]. Oma tarkvaraarendusprogrammi

[59] Google Inc. Letter to United States Securities and Exchange Commission on 20.12.2013, Re: Form 10-K for the fiscal year ended December 31, 2012. – www.sec.gov/Archives/edgar/data/1288776/000128877613000074/filename1.htm (17.02.2021).

[60] Heaks näiteks on Apple Watch, mille pulsisageduse mõõtmise rakendus viitas võimalikule südamerütmi häirele, mis ajendas kasutajat arsti poole pöörduma, päästes kasutaja nõnda võimalikust infarktist. See on suurepärane eesmärk ja teostus, kuid vastus küsimusele, kas selle isiku terviseandmeid peaks edastama ka reklaamivõrgustikele, on ilmselt eitav. Financial Express. How an Apple Watch possibly saved the life of this 58-year-old man. (05.02.2021) – https://www.financialexpress.com/industry/technology/how-an-apple-watch-possibly-saved-the-life-of-this-58-year-old-man/2188716/ (18.02.2021).

[61] Article 29 Data Protection Working Party. Opinion 8/2014 on the on Recent Developments on the Internet of Things. 14/EN, WP 223, 16.09.2014, lk 4; European Data Protection Supervisor. Opinion 6/2017. EDPS Opinion on the Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation). 24.04.2017, lk 9.

[62] Elcock, W. How to stop Google, Apple, and Microsoft from tracking your location. (07.08.2019) – https://www.comparitech.com/blog/vpn-privacy/stop-google-apple-microsoft-tracking-location/ (07.04.2021).

Facebook Software Development Kit (SDK) abil kogub Facebook andmeid nii konto omanike kohta, sõltumata sellest, kas nad on teenusesse sisse logitud või mitte, kui ka isikute kohta, kellel Facebooki kontot ei olegi[63] (vt ka juhiseid andmete Facebookile edastamise väljalülitamiseks[64]). Alates Facebooki loomisest 2004. aastal on Facebook patenteerinud tuhandeid jälgimist võimaldavaid tehnoloogiaid. Kuigi tehnoloogia patenteerimine ei taga selle toimivust päriselus ega kohusta patenteeritud tehnoloogiat kasutama, näitab see vähemalt sellise tehnoloogia kasutamise kaalumist. Facebooki esindajate väited, et Facebook on sageli patenteerinud tehnoloogiaid, mida nad kunagi ei rakenda ning et patendid ei viita tulevikuplaanidele, on käesoleva töö autori arvates võrdlemisi sisutühjad ja Facebooki „heale tahtele" lootmine sellises olukorras naiivne.[65]

Siin esitatud jälgimistehnoloogiate loetelu ei ole kaugeltki ammendav ning nende täpne defineerimine ei olegi andmekaitse kontekstis otstarbekas. Suurkorporatsioonide vahel käib kasumi nimel armutu tarkvarasõda ja pidev üksteise ületrumpamine: niipea kui leiutatakse viis blokeerida reklaame, kustutada küpsised või seadistada veebilehitseja jälgimist takistama, leitakse peagi võimalus neist mööda hiilida, muutes reklaamid raskemini tuvastatavaks ja salvestades küpsised teise kohta[66]. Omaette teemana võib jälgimistehnoloogiate kontekstis välja tuua mikrosuunamise (*microtargeting*)[67] või käitumise (mikro)nügimise (*nudging behaviour*)[68], mida kasutatakse mh poliitiliste protsesside varjatud suunamiseks ja isikutega manipuleerimiseks, mille tuntuim näide lähiminevikust on Cambridge Analytica skandaal.[69]

---

[63] Privacy International. How Apps on Android Share Data with Facebook (even if you don't have a Facebook account). 2018, lk 3–4.

[64] Carter, L. M. Facebook video on 23.02.2021. – https://www.facebook.com/LisaCarter247/videos/10224788418206327/ (14.03.2021).

[65] Näiteks patenteeris Facebook 2014. aastal USA-s tehnoloogia kasutajale sõbrasoovituste tegemiseks, mis võimaldab mobiiltelefonis oleva kiirendusanduri ja güroskoobi näitude põhjal tuvastada mitte üksnes selle, et isikud viibisid samas ajal ühes kohas, vaid ka selle, kas nad liikusid kõrvuti või olid vastamisi, mis võimaldab Facebookil soovitada kasutajale sõbraks isiku, kellega ta potentsiaalselt eelmisel õhtul klubis vestles, mitte iga isiku, kes tol õhtul klubis viibis. 2015. aastal patenteeris Facebook tehnoloogia, mis võimaldab seostada isikuid, kes laadivad üles sama kaameraga tehtud pilte, mis tuvastatakse nt pildi metaandmete (seerianumbri) või ka kaameraläätsel asuva tolmukübeme või kriimustuse põhjal. Mattu, S., Hill, K. Facebook Knows How to Track You Using the Dust on Your Camera Lens. (01.11.2018) – https://gizmodo.com/facebook-knows-how-to-track-you-using-the-dust-on-your-1821030620 (09.04.2021).

[66] Grimmelmann, J. Spyware vs. Spyware: Software Conflicts and User Autonomy. – Ohio State Technology Law Journal, Vol. 16, No. 1, Winter 2020, lk 27–33.

[67] American Association of Political Consultants. Alexander P. Gage. (*sine anno*) – https://theaapc.org/about-us/board-of-directors/alex-gage/ (21.02.2021).

[68] Käitumise nügimise termin loodi varem, kuid see sai populaarseks 2008. aastal selleteemalise raamatu avaldamisel. Thaler, R. H., Sunstein, C. R. Nudge: Improving Decisions About Health Wealth And Happiness. New Haven: Yale University Press, 2008.

[69] Amnesty International. Surveillance Giants: How the Business Model of Google and Facebook Threatens Human Rights. London: Amnesty International Ltd, 2019, lk 39–33; Commission of the European Communities. Communication from the Commission to the European Parliament and the Council. Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition – two years of application of the General Data Protection Regulation. COM(2020) 264 final. Brussels, 24.06.2020, lk 4.

1.3 Küpsiste ja muude jälgimistehnoloogiate tähtsus reklaamitööstuses

Infoühiskonnas nähakse andmeid kui omamoodi valuutat[70] või naftat[71], mis loovad jõukust. Võimalikult suur, esinduslik ja mitmekesine andmekogu on vajalik paljude uute tehnoloogiate, nagu suurandmetöötlus (*big data analysis*), tehisintellekt (*artificial intelligence*) ja masinõppe eri vormid (*machine learning*) arendamiseks ja neist saadava kasu maksimeerimiseks[72]. Nende tehnoloogiate võimalikud rakendusvaldkonnad katavad pea kõiki tegevusvaldkondi alates teadusest, meditsiinist ja põllumajandusest kuni justiitssüsteemi, finantsteenuste ja turunduseni[73]. Käesolevas töös keskendutakse viimasele ehk andmete olulisusele reklaamitööstuses ja turunduses.

Selleks et mõista reklaamitööstuses kasutatavaid ärimudeleid, tuleb esmalt anda ülevaade eri osapooltest ja nende rollist kaasaegses turundusprotsessis. Veebireklaam sarnanes algselt trüki- ja telereklaamile: reklaamija ja reklaamipinna omanik (nt veebisait) pidasid kahepoolseid läbirääkimisi reklaami kuvamiseks kokkulepitud tasu eest. Ent veebisaitide ning internetis toodete ja teenusepakkujate arvu kasvades polnud varsti enam mõeldav pidada otseläbirääkimisi kõigi koostööpartneritega, et veebisait saaks oma reklaamipinna võimalikult suures ulatuses tulu teenima panna ning reklaamija oma tooteid võimalikult laiale ostjaskonnale pakkuda. Veebisaidi ja reklaamija vahelist lünka asusid juba 1990. aastate keskel täitma reklaamivõrgustikud (*ad networks*), mille eesmärk oli leida reklaamijaid veebisaidi sellisele reklaamipinnale, mida veebisaidil polnud õnnestunud otse reklaamijatele müüa[74]. Seoses oksjonipõhise reklaami ostmise tehnoloogia arenguga 2000. aastate teises pooles[75] tulid turule internetireklaami tehnoloogiaettevõtted[76] (üldnimetusega *ad tech*), kes hakkasid looma automatiseeritud otsustus- ja analüüsiprotsesse ning tarkvara nn programmaatse ehk programmeeritult automaatse reklaami (*programmatic advertising*) esitamiseks. Kui algselt oli veebisaidi operaatorite ja reklaamijate vahel vaid üks lüli: reklaamivõrgustikud[77], siis hiljem on osapooli lisandunud. Sõltuvalt valitud mudelist võivad vahelülid olla järgmised: platvormid

[70] Kuneva; Langhanke, C., Schmidt-Kessel, M. Consumer Data as Consideration. – Journal of European Consumer and Market Law, Heft 6, 2015, lk 218.
[71] Council of Europe. European Commission for the Efficiency of Justice (CEPEJ), lk 18.
[72] Commission of the European Communities. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. A European strategy for data. COM(2020) 66 final. Brussels, 19.02.2020, lk 1–2.
[73] OECD, lk 47–71.
[74] Zawadziński, M. What Is an Ad Network and How Does It Work? Nt pakuvad reklaamivõrgustiku teenust Google AdSense, Google Display Network ja AdCash.
[75] Sweeney, M. What Is a Demand-Side Platform (DSP) and How Does It Work? The Clearcode Blog. (27.11.2020) – https://clearcode.cc/blog/demand-side-platform/ (22.02.2021).
[76] Viis tuntuimat reklaamitehnoloogia ettevõtet on Facebook, Amazon, Apple, Microsoft ja Alphabet Inc.'ile kuuluv Google (nn Big Five). Amnesty International, lk 10.
[77] Article 29 Data Protection Working Party. Opinion 2/2010 on online behavioural advertising. 00909/10/EN, WP 171, 22.06.2010, lk 5.

pakkumise poolel (*supply side platforms* ehk SSP), platvormid nõudluse poolel (*demand side platforms* ehk DSP), andmehaldusplatvormid (*data management platforms* ehk DMP), andmevahendajad (*data brokers*), reklaamivahendusplatvormid ehk reklaamibörsid (*ad exchanges*), reklaamivõrgustikud (*ad networks*) jne.[78] Üks turuosaline võib täita ka muude osapoolte funktsioone, nt käesoleval ajal on reklaamivõrgustike ja pakkumise platvormide (SSP) rollid ühte sulamas[79].

Pakkumise platvormid (SSP) aitavad reklaamipinna pakkujal hallata, müüa ja optimeerida oma reklaamipinda, mh valida algoritmide alusel paljude reklaamijate seast välja need, kes reklaamipinna eest kõige kõrgemat tasu maksavad[80]. Nõudluse platvormid (DSP) aitavad reklaamijal valida paljude reklaamipindade seast välja need, mis aitavad reklaamijale kõige sobivamate võimalike ostjateni jõuda. Nõudluse platvorm on nagu börsimaakler, kes ostab investori (reklaamija) nimel aktsiaid (reklaamipinda) börsil (reklaamivahendusplatvormil).[81] Selleks et valida välja reklaamijale parimad pakkumised, kasutavad nõudluse platvormid andmehaldusplatvorme (DMP) ja andmevahendajaid, kes koostavad mitmesugustest allikatest pärineva teabe põhjal ja erinevate tehnoloogiate abil turusegmente ja kasutajaprofiile ning müüvad seda teavet igale soovijale[82]. Veebisaidi operaator läbi SSP ja reklaamija läbi DSP kohtuvad reklaamibörsil[83].

Reklaamibörse on arendatud käsikäes viimase kümne aasta jooksul populaarsust kogunud ja tänaseks ühe levinuma ärimudeliga, milleks on reklaami ostmine oksjonipõhiselt reaalajas (*real-time bidding* ehk RTB)[84]. Kui varem maksid reklaamijad reklaami eest fikseeritud hinda kokkulepitud arvu näitamiste eest teatud ajavahemikus teatud veebisaidil, siis reklaami ostmine reaalajas toimuval oksjonil on suunatud sihtrühma külastajatele paljudel veebisaitidel, mitte reklaamipinna ostmisele konkreetsel veebisaidil[85]. Teisisõnu pole

[78] Geradin, D., Katsifis, D. An EU competition law analysis of online display advertising in the programmatic age. – European Competition Journal, Vol. 15 No. 1, 2019, lk 60–65.
[79] Zawadziński, M. What Is an Ad Network and How Does It Work?
[80] Zawadziński, M., Wlosik, M. What Is a Supply-side Platform (SSP) and How Does It Work? The Clearcode Blog. (25.11.2020) – https://clearcode.cc/blog/what-is-supply-side-platform/ (22.02.2021). SSP teenuseid pakuvad nt Google Doubleclick Ad Exchange (also known as AdX), PubMatic, AppNexus, ONE by AOL, OpenX ja The Rubicon Project.
[81] Sweeney. DPS teenuseid pakuvad nt Google DoubleClick Bid Manager, MediaMath ja Amazon DSP.
[82] Zawadziński, M. What is a Data Management Platform (DMP) and How Does it Work? The Clearcode Blog. (27.11.2020) – https://clearcode.cc/blog/data-management-platforms/ (22.02.2021). DMP teenuseid pakuvad nt BlueKai (Oracle), Weborama, Adobe Audience Manager, Acxiom, Experian ja Equifax.
[83] Geradin, Katsifis, lk 64. Reklaamibörsi teenust pakuvad nt Google Ad Manager, AppNexus, The Rubicon Project, OpenX ja One by AOL.
[84] Geradin, Katsifis, lk 61; van Eijk, R. J-W. Web Privacy Measurement in Real-Time Bidding Systems. A Graph-Based Approach to RTB system classification. Doctoral thesis. University of Leiden, 2019, lk 20.
[85] Krustok, I. Reaalajas reklaami ostmine. Gemius Estonia. (21.05.2015) – https://www.gemius.ee/468/reaalajas-reklaami-ostmine.html (22.02.2021).

reklaamija jaoks enam niivõrd oluline mitte kus, vaid kellele tema reklaami esitatakse ehk fookus on liikunud veebisaidi reklaamipinnalt veebisaidi külastajale[86].

Seda protsessi illustreerib Joonis 4, mille lugemist tuleb alustada paremalt ehk veebisaidi (skeemil *publisher*) ja kasutaja (*website visitor*) juurest. Ajal, mil kasutaja veebilehitseja laeb veebilehte, saadab reklaamipinna pakkuja (ehk veebisait) SSP kaudu välja pakkumise reklaami kuvamiseks (kas otse või reklaamibörsi vahendusel), misjärel DSP analüüsib andmeid ja reklaamija ette antud parameetreid ning valib külastaja profiili alusel välja reklaamijale sobivaimad reklaamipinnad ja teeb neile panused. Kui panus osutub valituks, saadab DSP reklaamija (*advertiser*) reklaami veebisaidile. Kogu see protsess toimub automatiseeritult ja algoritmide abil kiiremini kui silmapilgutus ehk umbes 0,1–0,3 sekundi jooksul (silmapilgutusele kulub hinnanguliselt 0,1–0,4 sekundit[87]).[88]

Joonis 4. Reklaamitööstuses osalejad

Allikas: Sweeney.

Ülaltoodud reklaamitööstuses osalejate liigitus ei ole ammendav ning turuosalisi on igas kategoorias arvukalt. Iga osapool saab valida endale sobivatel tingimustel koostööpartnereid (vähemalt teoreetiliselt[89]), täita mõnda funktsiooni ise või etappe soovi korral vahele jätta ja koostööpartneriga otse suhelda, mis teeb reklaamitööstuse väga dünaamiliseks. Samas on just turuosaliste paljusus, nendevaheliste rollide hägustumine ja kohatine kattuvus ning reklaamitehnoloogia kiired ja ettearvamatud arengud muutnud süsteemi sedavõrd keeruliseks, et isegi valdkonnateadlik turuosaline peab pidevalt valvel olema[90].

Kõiki neid osapooli ühendab siiski see, et nende kõigi huvides on võimalikult suures ulatuses üksikasjalik, täpne, asja- ja ajakohane teave reklaami sihtrühma ja iga üksiku kasutaja kohta. Andmevahendajad koguvad teavet ametlikest registritest (rahvastikuandmed, varad,

[86] Geradin, Katsifis, lk 61–62.
[87] B10 NUMB3R5. The Database of Useful Biological Numbers. Average duration of a single eye blink. – https://bionumbers.hms.harvard.edu/bionumber.aspx?&id=100706&ver=4 (22.02.2021).
[88] Sweeney.
[89] Õiguskirjanduses on leitud – ning see näib keskmisele kasutajale ilma uurimatagi nõnda – et Google valitseb õige mitut kirjeldatud turgu, mistõttu väiksemad turuosalised on oma valikutes vähem vabad. Geradin, Katsifis, lk 93–94.
[90] Geradin, Katsifis, lk 62.

tegevusload, sõiduki juhtimise load, äritegevus, kutsetunnistused, kohtuteave), koostööpartneritelt (tehinguandmed, kliendiandmed ja -programmid kaubanduses), muudest avalikest allikatest, sh kasutaja enda poolt sisestatuna (meedia, küsimustikud, uuringud, sotsiaalmeedia ja -võrgustikud) ning kasutaja jälgimise teel saadud andmetest (veebisaidid, mobiilirakendused, nutiseadmed)[91]. Mida kvaliteetsem on kasutaja kohta teadaolev informatsioon, seda kõrgemat hinda on reklaamija nõus oma sihtrühma kuuluva kasutaja eest maksma, mis omakorda tähendab suuremat tulu reklaamipinna omanikule. Ning vastupidi, kui reklaamijal on veebisaidi külastaja kohta vähe teavet, teeb ta väiksema panuse, kuna tegemist on n-ö põrsas kotis olukorraga.[92]

Andmete olulisusest kõnelevad ka reklaamitööstuse turgu valitsevate Google'i ja Facebooki majandusnäitajad: 2019. aastal moodustas üle 83% Google'i kogutulust reklaamitulu[93]; Facebooki puhul moodustas reklaamitulu 2019. aastal kogutulust koguni 98%. Kui Facebook ja Google teenivad oma põhitulu reklaamivahendamisest ning reklaamijad eelduslikult oma teenuste ja toodete müümisest, siis oluliselt haavatavamad on reklaamipindade omanikud, kes pakuvad oma põhiteenuseid tasuta. Paljude väikeste ja keskmise suurusega veebisaitide ja mobiilirakenduste jaoks on reklaamitulu ainus või oluline sissetulekuallikas tehingu- või tellimuspõhise tulu kõrval[94]. Mõnedel andmetel ei oleks isegi juhtivad uudisteportaalid ilma reklaamituluta majanduslikult tasuvad[95].

Õigusliku regulatsiooni muudatus, mis raskendab isikuandmete kättesaadavust ja töötlemist, olgu nõusoleku nõude või jälgimist keelavate vaikeseadete rakendamise teel, teeb suunatud reklaamil põhineva ärimudeli viljelemise väga keeruliseks. Regulatsiooni karmistumise tagajärjel võivad mitmed kasutaja jaoks praegu tasuta teenused muutuda

---

[91] United States Senate, Committee on Commerce, Science, and Transportation. Office of Oversight and Investigations Majority Staff. A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes. Staff Report for Chairman Rockefeller. (18.12.2013) – https://www.govinfo.gov/content/pkg/CHRG-113shrg95838/html/CHRG-113shrg95838.htm (16.03.2021), lk 15–21; Ramirez, E. jt. Data Brokers: A Call for Transparency and Accountability. USA: Federal Trade Commission, 2014, lk 11–14.

[92] Geradin, Katsifis, lk 62.

[93] Alphabet Inc. Annual Report Pursuant to Section 13 or 15(D) of the Securities Exchange Act of 1934 for the Fiscal Year Ended December 31, 2019. – https://www.sec.gov/Archives/edgar/data/1652044/000165204420000008/goog10-k2019.htm#s7E164D6797425D368E0A2E18504CF241 (20.02.2021), Item 1A; Facebook, Inc. Annual Report Pursuant to Section 13 or 15(D) of the Securities Exchange Act of 1934 For the Fiscal Year Ended December 31, 2019. – https://www.sec.gov/Archives/edgar/data/1326801/000132680120000013/fb-12312019x10k.htm#s54AFD3C4F459576CAFAC623F7B94CED5 (20.02.2021), lk 56.

[94] Scherb, M. Free Content's Future: Advertising, Technology, and Copyright. – Northwestern University Law Review, Vol. 98, No. 4, 2004, lk 1787–1788; Sherman, F. What Does Advertising-Supported Revenue Model Mean? Small Business. Chron. (08.12.2020) – https://smallbusiness.chron.com/advertisingsupported-revenue-model-mean-63332.html (23.02.2021); CookiePro. Website Tracking Technologies.

[95] Geradin, Katsifis, lk 84.

tasuliseks, kaotada kvaliteedis või kaduda turult sootuks.[96] Ühest küljest on majanduskäibes loomulik, et teenuse eest tuleb tasuda. Teisalt kui internetisisu on (vähemalt suures ulatuses) olnud kasutaja jaoks põhimõtteliselt interneti loomisest alates tasuta, on kaheldav, kas inimesed oleksid valmis hakkama Google'i või Facebooki konto kasutamise eest maksma, kuigi ajakirjandustellimuste, professionaalsete võrgustike (nt LinkedIn) ja teenuste (nt e-krediidiinfo) ning võrgu- ja mobiilimängude eest tasutakse. Faktiliselt maksavad inimesed paljude tasuta teenuste eest oma isikuandmetega[97] (*data as counter-performance, consideration*), kuigi õiguslikult selle üle vaieldakse, kas isikuandmeid saab pidada vastutasuks teenuse eest[98]. Reklaamitööstuse eestkõnelejad juhivad tähelepanu ka sellele, et rangemad reeglid vähendavad tõenäoliselt EL-i konkurentsivõimet võrreldes teiste regioonidega olukorras, kus suurimad meediatööstuse hiiud juba asuvad EL-ist väljaspool, eeskätt USA-s[99]. Ka Euroopa Komisjon möönab uue määruse ettepaneku mõjuhinnangus, et e-privaatsuse regulatsiooni muudatused mõjutavad tugevamalt väikseid ja keskmise suurusega ettevõtjaid[100].

Üldiselt on siiski lootust, et vastandlike huvidega osapooled suudavad üha enam tunnustada üksteise huve ja õigusi. Näiteks reklaamitööstuse huvide eest seisev Interactive Advertising Bureau (IAB), selgitab, et andmekaitse regulatsiooni karmistudes peavad reklaamijad leidma uusi viise klientideni jõudmiseks ja äritegevuse jätkamiseks. Organisatsioon möönab, et reklaamitööstuses on innovatsioon jõudnud ette regulatsioonist, kuid nüüd tuleb leida kooskõla privaatsuse, tarbijakaitse ja kogukonna huvide vahel.[101] E-privaatsuse määruse ümber toimuva arutelu üks tulipunkte ongi tasakaal ettevõtlusvabaduse ja põhiõiguste vahel eraelu puutumatusele ja isikuandmete kaitsele. Eri huvigruppide surve ja poliitilise konsensuse puudumine on peamised põhjused, miks e-privaatsuse määruse vastuvõtmine on oodatust kauem aega võtnud.

Vahel esitatakse andmekaitse aktivistidele vastuväide, et kui isik ei tee midagi valesti, siis pole tal ka midagi varjata ega põhjust jälgimist iga hinna eest karta. USA krüptograaf ja

---

[96] Interactive Advertising Bureau Europe (IAB). Position on the proposal for an ePrivacy Regulation. (28.03.2017) – https://iabeurope.eu/knowledgehub/policy/iab-europe-position-paper-position-on-the-proposal-for-an-eprivacy-regulation/ (21.02.2021), lk 4.

[97] Amnesty International, lk 9.

[98] Euroopa andmekaitseinspektori arvates ei või isikuandmeid pidada vastusoorituseks teenuse eest. Õiguskirjanduses leitakse vastupidist ning arutletakse, kuidas selliseid lepinguid lepingu- ja tarbijaõiguslikult reguleerida. European Data Protection Supervisor. Opinion 6/2017, lk 25; Helberger, N., Zuiderveen Borgesius, F. J., Reyna, A. The Perfect Match? A Closer Look at the Relationship Between EU Consumer Law and Data Protection Law. – Common Market Law Review, Vol. 54, No. 5, 2017, lk 1464; Langhanke jt, lk 222–223.

[99] Specht, L., Kerber, W. Datenrechte – Eine Rechts- und Sozialwissenschaftliche Analyse im Vergleich Deutschland – USA. Germany: ABIDA, 2018, lk 136–137.

[100] European Commission. Impact Assessment accompanying the document Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications). SWD(2017) 3 final. Part 1/3. Brussels, 10.01.2017, lk 39.

[101] Interactive Advertising Bureau Europe (IAB). – https://www.iab.com/topics/privacy/ (21.02.2021).

infoturbe ekspert Schneier argumenteerib, et see vastuväide lähtub eeldusest, et eraelu puutumatus on seotud mingisuguse pahateo varjamisega. See eeldus ei pea paika. Eraelu puutumatus on inimõigus ja väärib kaitset selle olemusest tulenevalt[102]. Ka teised autorid on selgitanud, et pidev jälgimine viib vaba eneseväljenduse piiramise ja enesetsensuurini[103]. Enam kui sada aastat tagasi ütles Inglismaa kohtunik J. Peterson ühes intellektuaalomandit puudutavas vaidluses 1916. aastal, et mis on väärt loata kopeerimist, see on *prima facie* väärt kaitsmist[104]. Sama võiks öelda andmete kohta: mis on väärt loata kasutamist, on väärt kaitsmist.

Käesolevas peatükis kirjeldati küpsiste ja muude jälgimistehnoloogiate olemust ja tehnilist toimimist ning nende kasutamist reklaamitööstuses käitumispõhise reklaami esitamiseks. Vastusena esimesele uurimisküsimusele saab öelda, et küpsis on kodeeritud tekstifail, mille veebisait (tehniliselt võttes server, kus veebisaiti hoitakse) salvestab kasutaja arvutisse mitmesugustel vajalikel või kasutaja jaoks otseselt mittevajalikel eesmärkidel. Reklaamivõrgustikud salvestavad küpsiseid sageli selliselt, et kui kasutaja külastab reklaame sisaldavat veebilehte (nt uudisteportaali), siis iga üksiku reklaami kuvamiseks saadab veebilehitseja päringu vastavat reklaami hoiustavale serverile, kes saadab vastu küpsise, mis salvestatakse kasutaja arvutisse, või täiendab kasutaja kohta juba olemasolevat küpsist teabega, et kasutaja on vastavat reklaami näinud. Kuigi küpsised on käesoleva töö kirjutamise ajal üheks levinumaks kasutajate veebitegevuse jälgimise vahendiks, saab kasutaja kohta andmeid koguda ka muul viisil, nt IP-aadressi, jälgimispikslite või ultrahelisignaalide abil. Kuigi teatud juhtudel on küpsised ja muud jälgimistehnoloogiad vajalikud ja kasulikud, nt asukoha jälgimine Google Maps'is sõidujuhiste saamiseks või kasutaja tervisenäitajate jälgimine nutikella abil, võib selliste andmete reguleerimata töötlemine tuua kaasa isiku eraelu puutumatuse riive. Teisalt on kasutajate kohta võimalikult paljude ja mitmekesiste andmete kogumine aluseks mitmesaja miljardilisele reklaamiärile, mis võimaldab paljudel veebisaitidel pakkuda meile internetis tasuta teenuseid. Nende huvide vahel tasakaalu leidmist käsitletakse töö viimases peatükis, kuid enne uuritakse järgmises peatükis, kuidas on küpsiste ja muude jälgimistehnoloogiate kasutamist EL-is siiani reguleeritud ja milline on käesoleva töö kirjutamise ajal kehtiv regulatsioon.

[102] Schneier, B. The Eternal Value of Privacy. (18.05.2006) – https://www.schneier.com/essays/archives/2006/05/the_eternal_value_of.html (17.02.2021).
[103] Zuiderveen Borgesius, Steenbruggen, lk 293, 298–300.
[104] *University of London Press Ltd* v *University Tutorial Press Ltd. Chancery Division*, [1916] 7 WLUK 79.

2 Küpsistele (*cookies*) ja muudele jälgimistehnoloogiatele kohalduv regulatsioon kehtiva e-privaatsuse direktiivi järgi

2.1 E-privaatsuse direktiivi seosed isikuandmete kaitse üldmäärusega

Et e-privaatsuse direktiiv käsitleb juba pealkirja järgi „isikuandmete töötlemist ja eraelu puutumatuse kaitset elektroonilise side sektoris", on ePD tihedalt seotud isikuandmete kaitse üldmäärusega (IKÜM), mille asemel kehtis varasemalt andmekaitsedirektiiv 95/46/EÜ[105] ning Euroopa elektroonilise side seadustikuga[106] (ESD), mille asemel kehtis varem elektrooniliste sidevõrkude ja -teenuste raamdirektiiv 2002/21/EÜ[107]. Need õigusaktid on otseselt mõjutanud ePD sisu ja tõlgendamist. Küpsiste kasutamise seisukohalt on oluline ePD suhe just isikuandmete kaitse üldmäärusega.

Juba ePD-le eelnenud isikuandmete töötlemist ja eraelu puutumatust telekommunikatsioonisektoris käsitlev direktiiv 97/66/EC[108] toetus suures osas andmekaitsedirektiivi terminitele (1997. aasta direktiivi art 1 lg 2 ja art 2). Sarnaselt sätestab ePD, et ePD sätted „täpsustavad ja täiendavad direktiivi 95/46/EÜ sätteid lõikes 1 nimetatud eesmärkidel" ning et „[k]ui ei ole sätestatud teisiti, kohaldatakse direktiivis 95/46/EÜ (...) sätestatud mõisteid" (ePD art 1 lg 2 ja art 2). E-privaatsuse direktiivi artikli 1 lg-s 1 nimetatud eesmärkideks on „põhiõiguste ja -vabaduste, eelkõige eraelu puutumatuse kaitse võrdväärse taseme [tagamine] isikuandmete töötlemise puhul elektroonilise side sektoris". Fraas „täiendab ja täpsustab" viitab esmapilgul selgelt ja arusaadavalt *lex specialis derogat legi generali* põhimõttele, kuid nende kahe õigusakti vaheline suhe on siiski nüansirikkam, kohati ebaselge ja seetõttu ka kriitikat pälvinud[109], mistõttu vääriks see teema tervikuna eraldi tähelepanu, kuid

[105] 24. oktoobri 1995. aasta Euroopa Parlamendi ja nõukogu direktiiv 95/46/EÜ üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta. – EÜT L 281, 23.11.1995, lk 31–50 (eestikeelne eriväljaanne: ptk 13 kd 15, lk 355–374).

[106] 11. detsembri 2018. aasta Euroopa Parlamendi ja nõukogu direktiiv (EL) 2018/1972, millega kehtestatakse Euroopa elektroonilise side seadustik. – ELT L 321, 17.12.2018, lk 36–214.

[107] 7. märtsi 2002. aasta Euroopa Parlamendi ja nõukogu direktiiv 2002/21/EÜ elektrooniliste sidevõrkude ja -teenuste ühise reguleeriva raamistiku kohta (raamdirektiiv). – EÜT L 108, 24.04.2002, lk 33–50 (eestikeelne eriväljaanne: ptk 13, kd 29, lk 349–366).

[108] Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector. – OJ L 24, 30.01.1998, lk 1–8.

[109] Debusseré, F. The EU E-Privacy Directive: A Monstrous Attempt to Starve the Cookie Monster. – International Journal of Law and Information Technology, Vol. 13, No. 1, 2005, lk 81–82; Specht, Kerber, lk 130, 139. Spindler, G. Klarheit für Cookies. – Neue Juristische Wochenschrift, Heft 35, 2020, lk 2516; Böhm, W-T., Halim, V. Cookies zwischen ePrivacy und DS-GVO – was gilt? – MultiMedia und Recht, Heft 10, 2020, lk 651; European Data Protection Board (EDPB). Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities. 12.03.2019, lk 4; Zuiderveen Borgesius, F. J. Personal data processing for behavioural targeting: which legal basis? – International Data Privacy Law, Vol. 5, No. 3, 2015, lk 163.

jääb väljaspoole käesoleva töö fookust. Käesoleva töö seisukohalt on siiski oluline analüüsida ePD ja IKÜM-i vahelisi suhted seoses kehtiva nõusoleku andmise tingimuste ja andmete töötlemise võimalike õiguslike alustega.

E-privaatsuse direktiivi artikli 2 p f sätestab, et „nõusolek, mille annab kasutaja või abonent, vastab direktiivis 95/46/EÜ määratletud andmesubjekti nõusolekule". Andmekaitsedirektiivi artikli 2 p h järgi on andmesubjekti nõusolek „iga vabatahtlik, konkreetne ja teadlik tahteavaldus, millega andmesubjekt annab nõusoleku töödelda tema kohta käivaid andmeid". Andmekaitsedirektiivi artikli 7 p a järgi peab andmesubjekti nõusolek olema ühemõtteline. Artikli 29 andmekaitse töörühm juhtis 2013. aastal just küpsiste kontekstis eraldi tähelepanu sellele, et nõusolek peab olema antud ühemõttelise aktiivse tegevusega, nagu nupule või lingile vajutamine või lahtri märgistamine. Tegevusetus ei tähenda kehtiva nõusoleku andmist ning nõusoleku andmine peab olema jälgitav ja seostatav konkreetse kasutajaga.[110]

Samamoodi tõlgendas viidatud sätteid Euroopa Liidu Kohus, kes leidis 2019. aastal tehtud *Planet49*[111] lahendis, mis käsitles 2013. aastal (st andmekaitsedirektiivi kehtimise ajal) toimunud sündmusi. Kohus leidis, et nõusolek küpsiste salvestamiseks, mis on antud eeltäidetud märkeruudu abil, millest kasutaja peab nõusoleku andmisest keeldumiseks märke eemaldama, ei ole antud kehtivalt. Kohus selgitas, et olukorras, kus kasutaja jätab eeltäidetud märkeruudu tühjendamata, „on praktiliselt võimatu objektiivselt kindlaks teha, kas ta on nõustunud oma isikuandmete töötlemisega, ning ammugi mitte, kas see nõusolek on antud teadlikult."[112] Et eelotsust taotlenud kohus pidi lahendama ka tulevikku suunatud rikkumise lõpetamisega seotud küsimuse, kohaldas kohus samasuguse tulemusega ka lahendi tegemise ajal kehtinud IKÜM-i.

2018. aastast kohalduma hakanud IKÜM on kehtivale nõusolekule esitatavate tingimuste osas rangem kui andmekaitsedirektiiv, nähes ette, et andmesubjekti nõusolek on „vabatahtlik, konkreetne, teadlik ja ühemõtteline tahteavaldus, millega andmesubjekt kas avalduse vormis või selge nõusolekut väljendava tegevusega nõustub tema kohta käivate isikuandmete töötlemisega" (art 4 p 11). IKÜM-i pp-is 32 on selgelt öeldud, et nõusolek tuleks anda selge kinnitusena, mis „võiks hõlmata vajaliku lahtri märgistamist veebisaidil, infoühiskonna teenuste tehniliste seadmete valimist või muud avaldust või käitumist, millest selles kontekstis konkreetselt nähtub andmesubjekti nõusolek teda puudutavate isikuandmete

[110] Article 29 Data Protection Working Party. Working Document 02/2013, WP 208, lk 4–5.
[111] EKo C-673/17, *Planet49 GmbH* versus *Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV*, ECLI:EU:C:2019:801, p 65. Selle lahendiga seoses tuleb märkida, et üks põhjustest, miks see vaidlus EL-i kohtuni jõudis, peitub tõsiasjas, et Saksamaa on üks neist liikmesriikidest, kes ei näinud vajadust 2009. aastal ePD-s tehtud muudatust – küpsise salvestamiseks aktiivse nõusoleku nõuet – riigi õigusesse üle võtta ega ole seda teinud tänini. Spindler, lk 2515; Böhm, Halim, lk 652.
[112] C-673/17, *Planet49*, p 55.

kavandatavaks töötlemiseks. Vaikimist, eelnevalt märgistatud lahtreid või tegevusetust ei tohiks seega pidada nõusolekuks." Eelöeldu tähendab, et viite kaudu IKÜM-ile esitab kehtiv ePD nõusolekule sama kõrged nõudmised kui IKÜM.

E-privaatsuse direktiivi ja IKÜM-i vahelise suhte määratlemine on oluline ka andmete töötlemise seaduslikkuse seisukohalt. E-privaatsuse direktiivi pp-is 10 selgitatakse, et „[e]lektroonilise side sektoris kohaldatakse direktiivi 95/46/EÜ eelkõige kõigil põhiõiguste ja -vabaduste kaitsmisega seotud juhtudel, mis ei kuulu täpselt käesoleva direktiivi kohaldamisalasse, sealhulgas vastutava töötleja kohustuste ja üksikisiku õiguste puhul." Üks juhtum, kus ePD kui *lex specialis* täpsustab IKÜM-i kui *lex generalis*'t, puudutab andmete töötlemise õiguslikke aluseid. IKÜM sätestab kuus õiguslikku alust isikuandmete töötlemiseks, nende seas nõusolek ja töötleja õigustatud huvi (IKÜM art 6 lg 1 p a–f), mis on ilmselt peamised reklaamitööstuse poolt kasutatavad töötlemise alused[113]. E-privaatsuse direktiiv seevastu lubab andmeid töödelda vaid nõusoleku korral ja sedagi piiratud juhtudel. Eelnev tähendab, et juhtudel, kus ePD näeb ette konkreetse õigusliku aluse andmete töötlemiseks, ei ole võimalik täiendavalt tugineda IKÜM-is sätestatud muudele õiguslikele alustele[114]. Sellisteks juhtudeks ePD-s on teabe salvestamine kasutaja lõppseadmesse või sellele juurde pääsemine (art 5 lg 3); metaandmete ja asukohaandmete töötlemine sideteenuste turundamiseks ja lisaväärtusteenuste osutamiseks (art 6 lg 1 ja 3, art 9 lg 1); ning otseturundus (art 13).

Lisaks sellele, et ePD sätestab andmete töötlemise ja küpsiste salvestamise alusena vaid nõusoleku (jättes kõrvale teenuse osutamiseks vajaliku töötlemise, mis võib toimuda nõusolekuta), juhitakse kirjanduses tähelepanu asjaolule, et ePD artikli 5 lg 3 kohane nõusolek (nõusolek küpsise salvestamiseks) ei ole samastatav IKÜM artikli 6 lg 1 p a kohase nõusolekuga (nõusolek isikuandmete töötlemiseks), sest need reguleerivad erinevat liiki toiminguid. Mõlemal juhul aga peab nõusolek vastama IKÜM-i nõuetele. Praktikas tähendab see seda, et nii küpsise salvestamiseks kui ka küpsisega kogutud andmete hilisemaks töötlemiseks peab olema nõusolek. See ei tähenda, et neid nõusolekuid ei võiks taotleda ühel ajal, kuid need peavad olema eristatavad.[115] Kui küpsise salvestamiseks on tarvis kasutaja nõusolekut ePD järgi, on suure tõenäosusega tarvis nõusolekut ka küpsiste kaudu saadud isikuandmete töötlemiseks IKÜM-i alusel[116].

---

[113] European Data Protection Board (EDPB). Guidelines 8/2020 on the targeting of social media users. Version 1.0. 02.09.2020, lk 14–15.

[114] Article 29 Data Protection Working Party. Opinion 03/2016 on the evaluation and review of the ePrivacy Directive (2002/58/EC). 16/EN, WP 240. 19.07.2016, lk 4; Article 29 Data Protection Working Party. Opinion 2/2010, WP 171, lk 10; European Data Protection Board (EDPB). Opinion 5/2019, lk 13–14.

[115] Zuiderveen Borgesius. Personal data processing for behavioural targeting, lk 173–175; Article 29 Data Protection Working. Opinion 02/2013 on apps on smart devices. 00461/13/EN, WP 202, 27.02.2013, lk 14.

[116] Information Commissioner's Office (ICO). Guidance on the use of cookies and similar technologies, lk 19–20, 22.

Enam-vähem sarnasel seisukohal on Böhm ja Halim, kes eristavad küpsistega seoses nelja töötlemise etappi: (1) töötlemine enne küpsise salvestamist; (2) küpsise salvestamine kasutaja lõppseadmesse; (3) küpsisele kui lõppseadmesse salvestatud teabele juurde pääsemine; (4) küpsise abil kogutud teabe edasine töötlemine. Böhm ja Halim leivad, et tulenevalt ePD artikli 5 lg 3 sõnastusest kohaldub ePD vaid teisele ja kolmandale etapile.[117] Esimese faasi töötlemine võiks seisneda nt veebisaidile jõudnud kasutaja veebilehitsejas ja/või konkreetsel veebisaidil tehtud tahteavalduse kontrollimises, eesmärgiga teha kindlaks, kas vastava kasutaja lõppseadmesse tohib küpsist salvestada (nii ka EK ja EN seisukohtade pp 21). Neljandas faasis tuleks määratleda, millist liiki andmetega (sisu-, meta-, asukoha-, isikuandmed) on tegu ja lähtuda vastavatest normidest.

Siinkohal võib tekkida küsimus, millal on küpsiste kaudu kogutavad andmed isikuandmed IKÜM-i mõttes. IKÜM-i artikli 4 p 1 järgi on isikuandmed „igasugune teave tuvastatud või tuvastatava füüsilise isiku („andmesubjekti“) kohta; tuvastatav füüsiline isik on isik, keda saab otseselt või kaudselt tuvastada”. Küpsis on tekstifail, mis võib paljudel juhtudel sisaldada isikuandmeid[118], olgugi et enamasti krüpteeritult[119]. Kui küpsis sisaldab kasutaja sisestatud kasutajatunnust ja parooli või kasutaja kohta loodud unikaalset identifikaatorit, on kindlasti tegemist isikuandmetega. Seejuures ei pea isik olema tuvastatav nimeliselt, piisab kui tuvastatav on konkreetne kasutaja[120]. Juhiseid selle kohta, millised andmed võivad osutuda isikuandmeteks, antakse IKÜM-is: „[f]üüsilise isiku tuvastatavuse kindlakstegemisel tuleks arvesse võtta kõiki vahendeid, mida vastutav töötleja või keegi muu võib füüsilise isiku otseseks või kaudseks tuvastamiseks mõistliku tõenäosusega kasutada” (IKÜM pp 26). Sellisteks vahenditeks võivad olla isikute seostamine „nende seadmete, rakenduste, tööriistade ja protokollide jagatavate võrguidentifikaatoritega, näiteks IP-aadresside või küpsistega, või muude identifikaatoritega, näiteks raadiosagedustuvastuse kiipidega” (IKÜM pp 30).

Küpsised võivad sisaldada andmeid nii kasutaja lõppseadme kohta kui ka muid veebikasutusega kaasnevaid andmeid, mida nimetatakse metaandmeteks[121]. Kasutades näitena Euroopa Andmekaitsenõukogu veebisaidil esitatud privaatsusteadet, saab küpsistega koguda

---

[117] Böhm, Halim, lk 653.
[118] Article 29 Data Protection Working Party. Working Document 02/2013, WP 208, lk 5–6; Digital Guide Ionos.
[119] All About Cookies. What information is in a cookie? (*sine anno*) – https://www.allaboutcookies.org/cookies/what-information-in-cookie.html (16.04.2021).
[120] Information Commissioner’s Office (ICO). Guidance on the use of cookies and similar technologies, lk 19; Article 29 Data Protection Working Party. Opinion 2/2010, WP 171, lk 9.
[121] Metaandmed on andmed, mida töödeldakse side edastamiseks elektroonilises sidevõrgus või sellise edastamisega seotud arveldamiseks (ePD art 2 p b). Arveldamiseks on metaandmeid vaja töödelda nt mobiili- või internetiteenuse lepingu alusel. Kehtiva ePD ja ESD kohaselt edastatakse sidet nt järgmiste rakenduste ja teenuste vahendusel: internetiühendus, (mobiil)telefoniteenused, internetipõhised isikutevahelist suhtlemist võimaldavad teenused, nagu Gmail, Skype, FaceTime, WhatsApp, Facebook Messenger, iMessage, Viber, Tinder (nim ka OTT-teenusteks, *Over-the-Top services*) (ePD art 2 p d; ESD art 2 p-d 4–5). Body of European Regulators for Electronic Communications (BEREC). Report on OTT services. BoR (16) 35, 2016.

järgmist teavet: IP-aadress (maskitud); asukoht: riik, piirkond, linn, ligikaudne laius- ja pikkuskraad (asukohatuvastus); päringu kuupäev ja kellaaeg (lehe külastamine); vaadatud lehe pealkiri; vaadatud lehe URL; enne käesolevat lehte vaadatud veebilehe URL; kasutaja seadme ekraani eraldusvõime; külastaja ajavööndi kellaaeg; failid, millel klõpsati ja mis alla laaditi; välisdomeenile viivad lingid, millel klõpsati; veebilehtede genereerimise aeg ehk lehe avanemiskiirus; kasutatava veebilehitseja põhikeel; brauseri versioon; brauseri pistikprogrammid (PDF, Flash, Java jne); operatsioonisüsteemi versioon ja seadme identifikaator; külastatud veebilehe keel; kampaaniad; otsingud veebilehel; ja sündmused.[122]

Euroopa Andmekaitsenõukogu veebisaidil kogutud andmeid kasutatakse külastajate tegevuse kohta anonüümsete statistiliste koondaruannete koostamiseks, st need ei sisalda (enam) isikuandmeid. Kõigi nende andmete analüüsimiseks kasutavad Euroopa Andmekaitsenõukogu ja muud Euroopa Komisjoni veebisaidid alates 2017. aastast teenust Europa Analytics, mis põhineb avatud lähtekoodiga[123] tarkvaral ning mida haldab täielikult Euroopa Komisjon[124]. Vaikimisi andmeid ei koguta, kasutajal on võimalus keelduda külastuse käigus enda isikuandmete kogumisest, anonüümimisest ja nende põhjal statistika koostamisest. Võrdluseks: 2019. aastal läbi viidud uuringus tuvastati, et 89% EL-i liikmesriikide ametlikest veebisaitidest ja 52% avalike tervishoiuteenuste veebisaitide esilehtedest sisaldavad kolmanda osapoole reklaamküpsiseid. Seda tehakse nt ametlikku veebisaiti integreeritud Youtube'i videote ja sotsiaalvõrgustike jagamise linkide (nn Facebooki „meeldib" nupu) vahendusel. Eesti Vabariigi Valitsuse veebisaidil www.valitsus.ee tuvastati kolmanda osapoole küpsised kolmest allikast: addthis.com (Oracle Corporation), doubleclick.net (Alphabet Inc.'ile kuuluv Google LCC), youtube.com (Alphabet Inc.).[125]

Kõik veebisaidid kahjuks nõnda eeskujulikud nagu EL-i institutsioonide veebisaidid ei ole. Nagu peatükis 1.3 kirjeldati, on andmevahendajate eesmärk just andmete laiaulatuslik kogumine ja kombineerimine, et üksikisik oleks tuvastatav. Varasemalt külastatud veebisaidid, nähtud reklaamid ja otsingumootorisse sisestatud sõnad on reklaamivahendajatele väga väärtuslik teave[126]. Kokkuvõttes on küpsiste puhul pigem tavaline, et tegemist on ühtlasi isikuandmetega ja tuleb kohaldada nii ePD-d kui ka IKÜM-i[127].

---

[122] European Data Protection Board (EDPB). https://edpb.europa.eu/cookies_et (17.04.2021).
[123] Avatud lähtekood on mistahes programmi, mille lähtekood on tehtud programmeerijatele ja kasutajatele kättesaadavaks nii kasutamiseks kui muutmiseks. Omandiõigusega kaitstud tarkvara tootjad üldiselt ei avalda lähtekoode. Avatud lähtekoodiga tarkvara töötatakse välja ja arendatakse koostöös avalikkusega ning see on saadaval tasuta. E-teatmik *sub vero* open source (1). – http://vallaste.ee/ (07.03.2021).
[124] European Union Agency for the Cooperation of Energy Regulators (ACER). EUROPA Analytics. (*sine anno*) – https://acer.europa.eu/Media/Pages/EUROPA-Analytics.aspx (17.04.2021).
[125] European Digital Rights (EDRi) and Cookiebot, 2019, lk 12.
[126] Digital Guide Ionos.
[127] European Data Protection Board (EDPB). Opinion 5/2019, lk 11.

See on andmetöötleja otsustada, kas ja milliseid küpsiseid ta kasutab, milliseid andmeid küpsiste abil kogub ja kuidas ta neid edasi töötleb. Olgu öeldud, et kasutaja veebitegevuse kohta võidakse andmeid koguda nii küpsiste kaudu kui ka muul viisil, millest mõnda käsitleti käesoleva töö peatükis 1.2 (nt asukoha tuvastamine ultrahelisignaali abil, kasutajale kuuluvate seadmete tuvastamine ühise IP-aadressi abil). Selliseid metaandmeid töötleb teenuse osutamise käigus ka teenuse osutaja. Nt Facebook ja Gmail võivad koguda teavet küpsiste teel, kuid nende kätte koguneb suur hulk sisu- ja metaandmeid ka kiirsõnumite ja e-kirjade edastamise tõttu; Google'i otsingumootor võib salvestada küpsiseid, kuid ta töötleb pidevalt ka kasutajate sisestatud otsisõnu ja klõpsatud linke[128]. Veebis surfamisel tekivad paratamatult külastuslogid[129], millele pääseb juurde veebisaidi haldaja ehk elektroonilise side teenuse osutaja, kuid mida võidakse salvestada ka küpsiste abil.

Käesolevas alapeatükis analüüsiti ePD seoseid IKÜM-iga ning toodi välja, et ePD toetub suures osas IKÜM-i sätetele, millest olulisim on IKÜM-i nõusoleku mõiste. Küpsiste kasutamisel peab arvestama sellega, et kõigepealt on tarvis küsida nõusolek kasutaja lõppseadmesse küpsise salvestamiseks ePD alusel ning seejärel on isikuandmete töötlemise korral vaja saada enamasti samuti nõusoleku IKÜM-i järgi. Järgnevalt käsitletakse 2002. aastal vastu võetud ePD sätteid küpsiste salvestamise kohta (ptk 2.2) ning 2009. aastal neisse sätetesse tehtud muudatusi (ptk 2.3).

2.2 Küpsistest loobumise võimalus (*opt out*)

Küpsiste ja muude jälgimistehnoloogiate regulatsioon kehtivas ePD-s on eeskätt seotud lõppseadme kaitsega, mis põhineb ePD artikli 5 lg-l 3. Põhjenduspunkti 24 järgi moodustavad „kasutajate lõppseadmed ja sellistes seadmetes säilitatav teave (...) osa kasutajate eraelust, mida tuleb kaitsta inimõiguste ja põhivabaduste kaitse Euroopa konventsiooni kohaselt." Küpsiseid kui üht konkreetset andmete kogumise tehnoloogiat ei mainita ePD artiklites, küll aga ePD preambulis (pp 25), mis viitab sellele, et küpsistest oli 2000. aastate alguseks kujunenud sedavõrd levinud viis isikute tegevuse jälgimiseks internetis, et peeti vajalikuks neile direktiivis eraldi tähelepanu pühendada. Seejuures oli ePD tõenäoliselt esimene küpsiseid reguleeriv õigusakt maailmas[130].

E-privaatsuse direktiivi artikli 5 lg 3 paneb liikmesriikidele kohustuse tagada, „et elektrooniliste sidevõrkude kasutamine teabe salvestamiseks või juurdepääsuks abonendi või kasutaja lõppseadmesse salvestatud teabele on lubatud ainult tingimusel, et asjaomasele

[128] European Data Protection Board (EDPB). Opinion 5/2019, lk 11.
[129] E-teatmik *sub vero* access log. – http://vallaste.ee/ (16.04.2021).
[130] Debusseré, lk 96.

abonendile või kasutajale esitatakse direktiivi 95/46/EÜ kohaselt selge ja arusaadav teave muu hulgas andmete töötlemise eesmärgi kohta ning talle antakse võimalus keelduda vastutava andmetöötleja teostatavast töötlemisest". Kuigi ePD artikli 5 lg-t 3 seostatakse enim just küpsistega, on säte sõnastatud laiemalt, reguleerides mistahes teabe salvestamist lõppseadmesse ja juurdepääsu sinna salvestatud teabele, kui see toimub elektroonilise side võrkude (nt interneti) kaudu.

Küpsiste puhul on lõppseadmesse salvestatavaks teabeks lühike tekstifail, mille veebisait esmakülastuse ajal kasutaja arvutisse salvestab ning mida sealt järgnevate külastuste ajal n-ö loeb ehk pääseb juurde lõppseadmesse juba salvestatud teabele. Lõppseadmes olevaks teabeks võib olla ka lõppseadme asukoht, kasutaja kontaktide loetelu[131], mobiilseadme puhul sageli ka pildid ja videod[132]. Seejuures ei eelda ePD artikli 5 lg 3, et tegemist oleks isikuandmetega, vaid säte kaitseb lõppseadet volitamata juurdepääsu eest igasugusele seadmes olevale teabele. Seda, et ePD artikli 5 lg 3 kohaldub sõltumata andmete liigist, on kinnitanud ka Euroopa Liidu Kohus asjas *Planet49*[133]. Keelatud on mõistagi ka igasuguse pahavara salvestamine kasutaja lõppseadmesse, millest ePD pp 24 mainib nuuskurvara, veebilutikaid ja varjatud identifikaatoreid, mis võimaldavad kasutaja teadmata jälitada tema tegevust ja sekkuda tema eraellu.

Artikli 5 lg 3 olulisim erinevus ePD muudest sätetest on see, et kui enamik ePD sätteid reguleerib üksnes elektroonilise side võrkude ja teenuste osutajate tegevust, siis lõppseadmesse teabe salvestamise ja sealt teabe lugemise keeld kehtib ilma eranditeta kõigile isikutele, kes küpsiseid ja sarnaseid tehnoloogiaid kasutavad, sh veebisaidi omanikele, infoühiskonna teenuste pakkujaile[134], suhtlusvõrgustikele, uudisteportaalidele ja reklaamivõrgustikele[135].

E-privaatsuse direktiivi artikli 5 lg 3 ei olnud direktiivi koostajate jaoks enesestmõistetav. Komisjon juhtis 2000. aastal ePD ettepaneku seletuskirjas küpsiste kasutamisele tähelepanu, kuid oli seisukohal, et direktiivi kaitset ei peaks laiendama elektroonilise side teenustelt ja võrkudelt lõppseadmele sh tarkvarale, vaid tuleks leida muid lahendusi[136]. Direktiivi menetlusdokumentidest nähtub, et parlament soovis lisada lõike 3

[131] Deloitte. Evaluation and review of Directive 2002/58 on privacy and the electronic communication sector. Final Report. A study prepared for the European Commission DG Communications Networks, Content & Technology. EU, 2017, lk 135.
[132] Article 29 Data Protection Working. Opinion 02/2013, WP 202, lk 14.
[133] C-673/17, *Planet49*, p 68–70.
[134] DLA piper UK LLP. Study on the revision of the ePrivacy Directive for ETNO (European Telecommunications Network Operator's Association). Brussels: DLA piper UK LLP, 2016, lk 29.
[135] Hogan & Hartson LLP, Analysys Consulting Ltd. Preparing the next steps in regulation of electronic communications. A contribution to the review of the electronic communications regulatory framework. Final Report. July 2006, lk 264–265.
[136] European Commission. Proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector. COM(2000) 385 final, 2000/0189(COD). OJ C 365 E, 19.12.2000, lk 223–229, lk 223–229, Explanatory Memorandum, ptk 4.

selliselt, et nähtamatute jälgimisvahendite, nagu küpsiste kasutamine oleks võimalik vaid kasutaja nõusoleku korral. Nõukogu, kiites küll heaks artiklisse 5 lõike 3 lisamise, asendas nõusoleku nõude teabe esitamise kohustuse ja loobumisõigusega (*right to refuse*), mis tähendab, et vaikimisi oli küpsiste kasutamine lubatud (*opt out*). Nõukogu põhjendas asendust sellega, et kuna jälgimistehnoloogiaid kasutatakse paljudel juhtudel elektroonilise side võrgus teenuste osutamise toetamiseks, võib eelneva nõusoleku nõudmine luua põhjendamatuid takistusi jälgimisvahendite selliseks kasutuseks. Nõukogu leidis, et kui kasutajaid on jälgimisvahenditest nõuetekohaselt teavitatud ja neile on antud võimalus sellest keelduda, siis on kasutajate privaatsusõiguste kaitsmise eesmärk saavutatud.[137]

Sellesse seisukohta tuleb suhtuda väga kriitiliselt. Esmalt võib „teenuste osutamise toetamine" sõltuvalt tõlgendajast hõlmata laia arsenali andmetöötlustoiminguid. Nt võiks uudisteportaali või veebipoe pidamist toetavaks pidada analüütika- ja funktsionaalsusküpsiste kasutamist[138] (nt küpsiste kaudu isiku keele-eelistuste ja asukoha salvestamine, mis on ptk-s 1.1 esitatud liigituse järgi tüübid 2 ja 3). Laiendava tõlgendamise korral võiks isegi väita, et teenuse osutamist toetab ka turundusküpsiste kasutamine, kuivõrd veebisaidi operaator teenib veebisaidil reklaamipinna pakkumisega tulu, mis võimaldab tal mh enda teenuseid osutada[139] (ptk-s 1.1 esitatud liigituse järgi tüüp 4).

Kummaline on aga nõukogu tehtud asendus artikli 5 lg 3 viimase lause valguses, mis sätestab, et teavitamise ja loobumisvõimaluse pakkumise kohustus „ei takista tehnilist salvestamist või juurdepääsu, mille ainus eesmärk on teostada *või toetada* side edastamist elektroonilises sidevõrgus või mis on hädavajalik sellise infoühiskonna teenuse osutamiseks, mida abonent või kasutaja on selgesõnaliselt taotlenud" (autori rõhutus). Teisisõnu artikli 5 lg 3 viimane lause juba võimaldab jälgimisvahendite kasutamist side edastamise toetamiseks, mistõttu ei tohiks andmetöötlejatele olla vaja veel üht erandit või alust. Komisjon aga pidas nõukogu parandust sobivaks kompromissiks parlamendi poolt ettepandu ja ettevõtjate seisukohtade vahel[140].

Artikli 5 lg 3 esimene lause, milles lubatakse salvestada lõppseadmesse teavet kasutaja teavitamise ja talle loobumisvõimaluse andmise tingimusel, annab andmetöötlejale hoopis

---

[137] Commission of the European Communities. SEC/2002/0124 final, ptk 3.2.2; Council of the European Union. Common Position adopted by the Council on 28 January 2002 with a view to the adoption of the Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector. Interinstitutional File: 2000/0189 (COD). 15396/2/01 REV 2 ADD 1. Brussels, 29.01.2002, lk 5.

[138] European Data Protection Supervisor. Opinion of the European Data Protection Supervisor on the Proposal for a Directive of the European Parliament and of the Council amending, among others, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). – OJ C 181, 18.07.2008, lk 10.

[139] European Data Protection Supervisor. Opinion 5/2016, lk 17.

[140] Commission of the European Communities. SEC/2002/0124 final, ptk 3.2.2.

laiema võimaluse teabe salvestamiseks kasutaja lõppseadmesse (teavitamise tingimusel) kui artikli 5 lg 3 teine lause, mis eeldab kas (1) salvestamise hädavajalikkust konkreetse infoühiskonna teenuse osutamiseks (*necessity clause*) või (2) eesmärgina side edastamise toetamist. Artikli 5 lg 3 esimene lause ei ütle midagi küpsise salvestamise eesmärgi kohta. Lisaks on selge, et aktiivse nõusoleku asendamine passiivse nõusolekuga on andmekaitse seisukohalt suur samm nõrgema kaitse suunas.

Vaikiva nõusoleku lubamisega ePD probleemid kahjuks ei piirdu. Põhjenduspunktis 25 antakse kaks andmekaitse seisukohalt küsitava väärtusega selgitust küpsiste jm selliste vahendite kasutamiseks. Esiteks selgitatakse, et teavet kasutaja lõppseadmesse salvestatavate erinevate jälgimisvahendite kohta ja võimalust neist keelduda võib pakkuda ühe korra ühe ja sama ühenduse ajal ning see võib hõlmata ka kõnealuste vahendite edaspidist kasutamist järgmiste ühenduste ajal. Sellest järeldub, et kui kasutaja on ühel korral küpsiste salvestamisega nõustunud, siis hilisemate ühenduste ajal talle enam loobumisvõimalust pakkuma ei pea, mis võib tähendada nõustumist ettenägematult pikaks ajaks. Loobumisvõimaluse ühekordne pakkumine, mis hõlmab ka järgmisi ühendusi, on loogiliselt vildakas ka seetõttu, et kui kasutaja on ühel korral keeldunud küpsise salvestamisest, siis kuidas teab veebisait järgmisel korral, et kasutaja on küpsistest keeldunud, kui ta ei või salvestada sellekohast teavet sisaldavat küpsist.[141] Artikli 29 andmekaitse töörühm on hiljem analüüsinud, kas kõnealust lauset võiks mõista nõnda, et ühel korral küpsise *salvestamisega* nõustumine hõlmab sellesama küpsise edaspidist *lugemist* kasutaja arvutist erinevate veebisaitide poolt, mitte aga järgmiste küpsiste salvestamist. Sellisel juhul ei peaks kasutajat teavitama ja loobumisvõimalust pakkuma iga kord, kui veebisait küpsist loeb, vaid ainult siis, kui see konkreetne küpsis kasutaja arvutisse salvestatakse, kuid üheselt selge see ei ole. Samuti ei ole pp 25 sõnastusest „võib hõlmata ka kõnealuste vahendite edaspidist *kasutamist*" (autori rõhutus) üheselt selge, mida selline „kasutamine" tähendab.[142]

Teiseks selgitatakse pp-is 25, et juurdepääsu teatavale veebisisule võib teha sõltuvaks küpsise või muu sellise vahendiga nõustumisest, kui küpsist vm sellist vahendit kasutatakse õiguspärasel eesmärgil. Õiguspärane eesmärk on väga lai mõiste ning ei ole seotud küpsise vajalikkusega konkreetse teenuse osutamiseks[143] (nt veebisisu kuvamiseks). Lisaks seondub tingimusliku juurdepääsuga küsimus, kas nõusolekut saab lugeda vabalt antuks IKÜM-i mõttes,

[141] Debusseré, lk 88–89.
[142] Article 29 Data Protection Working Party. Opinion 2/2010 on online behavioural advertising, lk 16.
[143] Debusseré, lk 89.

kui see on seatud sisule või teenusele juurdepääsu tingimuseks[144]. Seda küsimust käsitletakse ka käesoleva töö peatükis 3.3.

Lõppseadme kaitsega on seotud veel üks oluline teema: nimelt lõppseade ise ehk täpsemalt selle tark- ja riistvaralised omadused. Artikli 29 andmekaitse töörühm väljendas juba 1997. aastal muret privaatsuse ja anonüümsuse kadumise pärast andmete massilise, kiire ja odava kogumise, töötlemise ja edastamise kontekstis, kus klõpsude jada jätab igast isikust digijälje[145]. Töörühm oli eriti murelik töötlemise pärast, mis toimub kasutaja teadmata ja tema jaoks n-ö nähtamatult, mille näiteks on HTTP protokolli abil koos päringuga muu teabe edastamine (eeskätt küpsiste kujul) ja automaatselt laadivad hüperlingid kolmandate osapoolte veebisaitidele, mis teavitavad reklaamivõrgustikku kasutaja asukohast veebis. Töörühma seisukoht 1999. aastal oli, et tark- ja riistvara peaks vaikimisi mitte lubama küpsiste ja kasutaja seadmega seotud ja andmeside pidamiseks mittevajaliku teabe kogumist, töötlemist ja edastamist (hiljem IKÜM-i artiklist 25 tulenev vaikimisi andmekaitse, *privacy by default*). Kasutajal peaks küpsise salvestamisel ja saatmisel iga kord olema võimalus sellega nõustuda või sellest keelduda, sh filtreerida, milliseid andmeid ta lubab edastada. Ühtlasi julgustas töörühm tark- ja riistvaratootjaid looma tooteid ja teenuseid, mis vastavad EL-i andmekaitsereeglitele (hiljem IKÜM-i artiklist 25 tulenev lõimitud andmekaitse, *privacy by design*).[146]

Ka komisjoni ePD ettepaneku seletuskirjas mööndi andmekaitse lünklikkust olukorras, kus sideteenuse osutajal on kohustus tagada side turvalisus, konfidentsiaalsus ja metaandmete kustutamine, samas kui tarkvara, mis on vajalik vastava sideteenuse osutamiseks (veebilehitsejad, e-postirakendused), andmekaitse nõuetele ei vasta[147]. Komisjoni ettepaneku pp-i 22 ja vastu võetud ePD pp-i 46 järgi ei tohiks andmete kaitse sõltuda teenuse eri komponentide konfiguratsioonist, mistõttu „*võib osutuda vajalikuks* selliste meetmete võtmine, mis kohustaksid elektroonilisteks sideteenusteks kasutatavate teatavat liiki seadmete tootjaid konstrueerima oma tooted nii, et neisse oleks integreeritud vahendid, millega tagatakse kasutajate ja abonentide isikuandmete ja eraelu puutumatuse kaitse" (autori rõhutus). E-privaatsuse direktiivi artikli 14 lg 3 sätestab võimaluse võtta vajaduse korral vastu „meetmeid tagamaks, et lõppseadmete konstrueerimine on kooskõlas kasutajate õigusega kaitsta oma isikuandmeid ja kontrollida nende kasutamist" kooskõlas direktiiviga 1999/5/EÜ ja nõukogu

[144] Article 29 Data Protection Working Party. Opinion 8/2006 on the review of the regulatory Framework for Electronic Communications and Services, with focus on the ePrivacy Directive. 1611/06/EN, WP 126, 26.09.2006, lk 3.
[145] Article 29 Data Protection Working Party. Recommendation 3/97, lk 4.
[146] Article 29 Data Protection Working Party. Recommendation 1/99, lk 2–4.
[147] European Commission. Proposal. COM(2000) 385 final, lk 223–229, Explanatory Memorandum, ptk 4.

otsusega 87/95/EMÜ. Direktiivi 1999/5/EÜ[148] artikli 3 lg 3 p c järgi „*[k]omisjon võib* (...) otsustada, et teatavatesse seadmeklassidesse kuuluvad seadmed või konkreetset tüüpi seadmed peavad olema valmistatud sel viisil, et need sisaldavad turvaseadmeid, et tagada kasutajate ja abonentide isikuandmete ja eraelu puutumatuse kaitse" (autori rõhutus). Viimati nimetatud direktiiv käsitleb küll üksnes raadioseadmeid, kuid uue ePM-i järgi oleksid hõlmatud praktiliselt kõik sidet võimaldavad elektroonilised seadmed. Kokkuvõttes ei sätesta kumbki direktiiv tark- ja riistvaratootjatele siduvat kohustust soodustada isikuandmete kaitset juba toote või teenuse disainimisel.

Oma esimeses ülevaateraportis andmekaitsedirektiivi 95/46/EÜ rakendamise kohta (avaldatud 2003) ning teatises andmekaitse edendamise kohta eraelu puutumatust soodustavate tehnoloogiate kaudu[149] (*privacy enhancing technologies*) (avaldatud 2007) kirjutas komisjon, et nimetatud tehnoloogiad aitaksid kaasa kehtiva regulatsiooni eesmärkide, mh võimalikult väheste ja eelistatult anonüümitud või pseudonüümitud andmete kasutamisele sellega, et andmekaitsereeglite rikkumine poleks mitte üksnes keelatud ja sanktsioneeritud, vaid ka tehniliselt takistatud.[150] See võib kujuneda üheks vaidlusküsimuseks ka uue ePM-i menetlemisel (vt ptk 3.3).

2.3 Küpsistega nõustumise võimalus (*opt in*)

Küpsiste ja muude jälgimistehnoloogiate kasutamisega seoses tehti 2009. aastal põhimõtteline muudatus. 2002. aastal vastu võetud ePD artikli 5 lg 3 lubas andmetöötlejal kasutaja lõppseadmesse teavet salvestada või sinna salvestatud teabele juurde pääseda tingimusel, et kasutajale esitatakse selge ja arusaadav teave mh andmete töötlemise eesmärgi kohta ning talle

[148] 9. märtsi 1999. aasta Euroopa Parlamendi ja nõukogu direktiiv 1999/5/EÜ raadioseadmete ja telekommunikatsioonivõrgu lõppseadmete ning nende nõuetekohasuse vastastikuse tunnustamise kohta. – EÜT L 91, 07.04.1999, lk 10–28 (eestikeelne eriväljaanne: ptk 13 kd 23 lk 254–272).

[149] Privaatsust soodustavad tehnoloogiad on näiteks andmete automaatne anonüümimine, krüpteerimine ja küpsiste blokeerimine. Mitmed vähemtuntud suhtlusrakendused pakuvad sõnumite otspunktkrüpteerimise võimalust (*end-to-end encryption*), mille korral andmed krüpteeritakse lähtepunktis ja dekrüpteeritakse sihtpunktis, st teekonna vältel on andmed krüpteeritud. Üks populaarseim sellistest rakendustest oli kuni 2014. aastani WhatsApp, mil selle ostis Facebook, omandades nõnda ligipääsu vähemalt WhatsAppi metaandmetele. Käesoleva töö kirjutamise ajal on privaatsuse aspektist turvalisim valik Signal. Corrigan, C. The Very Best Encrypted Messaging Apps. AVG. (26.03.2020 updated on 18.01.2021) – https://www.avg.com/en/signal/secure-message-apps (14.03.2021); Nield, D., Turner, B. Best encrypted instant messaging apps of 2021 for Android. (13.01.2021) – https://www.techradar.com/best/best-encrypted-messaging-app-android (14.03.2021); Gordon, T. 10 Most Secure Messaging Apps – The Best Platforms & Solutions. (12.01.2021) – https://getstream.io/blog/most-secure-messaging-apps/ (14.03.2021).

[150] Commission of the European Communities. Report from the Commission. First report on the implementation of the Data Protection Directive (95/46/EC). COM(2003) 265 final. Brussels, 15.05.2003, lk 16; Commission of the European Communities. Communication from the Commission to the European Parliament and the Council on Promoting Data Protection by Privacy Enhancing Technologies (PETs). COM(2007) 228 final. Brussels, 02.05.2007, lk 3.

antakse võimalus töötlemisest keelduda. Direktiiviga 2009/136/EÜ[151] sisse viidud muudatuse järgi võib kasutaja lõppseadmesse teavet salvestada või sellele juurde pääseda üksnes kasutaja teadliku nõusoleku alusel. Ehk teisisõnu senine loobumisvõimalus (*opt out*) asendati nõustumisvõimalusega (*opt in*).

Vastuoluliselt on pp-is 66 viidatud siiski teavitamiskohustusele ja loobumisvõimaluse andmisele, mis ei tohiks artikli 5 lg 3 muudatuste kontekstis enam asjakohane olla. Selle vastuolu põhjus peitub asjaolus, et enne nõukogu poolt direktiivi 2009/136/EÜ vastuvõtmist allkirjastasid 13 liikmesriigi esindajad seisukoha, milles deklareerisid, et nagu nähtub põhjenduspunktist 66, ei kavatseta muudetud artikli 5 lõikega 3 muuta olemasolevat nõuet, et kõnealust nõusolekut väljendatakse õigusega keelduda küpsiste ja sarnaste tehnoloogiate kasutamisest. Nende kolmeteistkümne riigi seas oli ka Eesti.[152] See tähendab, et üle poole liikmesriikidest (13 riiki 22-st) ei olnud tegelikult loobumisvõimaluselt nõustumisvõimalusele ülemineku poolt ega plaaninud seda jõustada. Nõusoleku andmine rakenduse seadete kaudu saab ilmselt olema üks suuremaid uuendusi uues ePM-is.

Parlamendis esimesel lugemisel heaks kiidetud versioonis sisaldus artikli 5 lg-s 3 nõusolekuga seoses täpsustus, et „brauseri vastavad seaded kujutavad endast eelnevat nõusolekut"[153]. Vastu võetud direktiivi artikli 5 lg-s 3 seda täpsustust ei ole (st nõusolekule rakenduvad kõik IKÜM-i nõuded ePD art 2 üldise viite kaudu), kuid see mõte on viidud direktiivi 2009/136/EÜ preambulisse, mille pp 66 selgitab, et „[k]ui see on tehniliselt võimalik ja tulemuslik vastavalt direktiivi 95/46/EÜ asjakohastele sätetele, võib kasutaja nõusolek andmete töötlemisega väljenduda kohaste brauseri vm rakenduse seadete kasutamises." Seega

[151] 25. novembri 2009. aasta Euroopa Parlamendi ja nõukogu direktiiv 2009/136/EÜ, millega muudetakse direktiivi 2002/22/EÜ universaalteenuse ning kasutajate õiguste kohta elektrooniliste sidevõrkude ja -teenuste puhul, direktiivi 2002/58/EÜ, milles käsitletakse isikuandmete töötlemist ja eraelu puutumatuse kaitset elektroonilise side sektoris, ning määrust (EÜ) nr 2006/2004 tarbijakaitseseaduse jõustamise eest vastutavate siseriiklike asutuste vahelise koostöö kohta. – ELT L 337, lk 11–36.

[152] Council of the European Union. Adoption of the proposal for a Directive of the European Parliament and of the Council amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of electronic communications networks and services, and 2002/20/EC on the authorisation of electronic communications networks and services (LA + S) (third reading). Statements. Interinstitutional file: 2007/0247 (COD). 15864/09 ADD 1 REV 1. Brussels, 18.11.2009, lk 3. Muuseas Eesti Andmekaitse Inspektsioon hääletas ka EL-i andmekaitseasutusi ühendava artikli 29 andmekaitse töörühma arvamuse vastu, mis käsitles IKÜM-i reformi ettepanekut, sest nägi selles liiga palju murettekitavaid probleeme. Article 29 Data Protection Working Party. Opinion 01/2012 on the data protection reform proposals. 00530/12/EN, WP 191, 23.03.2012, lk 32.

[153] European Parliament legislative resolution of 24 September 2008 on the proposal for a directive of the European Parliament and of the Council amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on consumer protection cooperation (COM(2007)0698 – C6-0420/2007 – 2007/0248(COD)). Vastu võetud tekst: P6_TC1-COD(2007)0248. – OJ C 8 E, 14.01.2010, lk 386.

kehtiv ePD põhimõtteliselt siiski toetab nõusoleku andmist veebilehitseja seadete kaudu, erinevalt artikli 29 andmekaitse töörühmast[154].

Menetlusdokumentidest ei nähtu, et loobumisvõimaluse asendamist nõustumisvõimalusega oleks põhjalikult arutatud, kuid saab siiski järeldada, et selles küsimuses ei olnud kerge leida üksmeelt. Komisjoni ettepanek seda ei sisaldanud, parlamendis pakuti see välja, nõukogu ühine seisukoht oli jääda loobumisvõimaluse ja teavitamiskohustuse juurde[155], kuid lõpuks lepiti siiski kokku nõusoleku nõude rakendamises. 2009. aasta muudatused on põhjus, miks ePD-d hakati mitteametlikus kõnepruugis nimetama küpsiste seaduseks (*cookie law*), sest kuigi küpsiseid mainiti esimest korda juba 2002. aasta direktiivis, äratasid muudetud ePD-le järgnenud hüpikaknad küpsiste lubamise taotlustega peaaegu igal veebisaidil keskmise interneti kasutaja tähelepanu märksa rohkem kui pelgalt aktiivset tegevust mittenõudev teavitamine ja loobumisvõimaluse pakkumine.

Artikli 5 lg 3 teisest lausest kustutati menetluse käigus viide side edastamise toetamisele, mille tulemusena on ilma nõusolekuta lubatud vaid tehniline salvestamine või juurdepääs, mille ainus eesmärk on teostada (mitte lisaks ka toetada) side edastamist. Seda saab pidada positiivseks muudatuseks, sest nagu käesoleva töö peatükis 2.2 arutleti, võivad töötlejad „side edastamist toetavaid tegevusi" tõlgendada enda huvides ülemäära laialt. Ka Euroopa andmekaitseinspektor juhtis sellele tähelepanu oma arvamuses komisjoni esialgse ettepaneku kohta, märkides, et direktiiv ei selgita, mida side edastamise toetamise all silmas peetakse[156].

Kehtiva ePD järgi on artikli 5 lg 3 kohase nõusoleku küsimise ja teavitamise kohustustest tehtud kaks erandit: nõusoleku saamise ja teavitamise kohustust ei ole, kui (1) salvestamise ja juurdepääsu ainus eesmärk on edastada sidet (side edastamise erand), ning (2) salvestamine ja juurdepääs on teenuse osutajale hädavajalik sellise infoühiskonna teenuse osutamiseks, mida kasutaja on sõnaselgelt taotlenud (hädavajalikkuse erand)[157]. Mõlemad erandid on väga ranged. Side edastamise erand tähendab seda, et ilma teabe salvestamiseta ei oleks side edastamine võimalik. Nt kui kasutaja soovib külastada teatud veebilehte, saadab tema veebilehitseja päringu serverile, kus vastavat veebilehte hoitakse. Vastaval serveril on vaja

[154] Article 29 Data Protection Working Party. Opinion 1/2009 on the proposals amending Directive 2002/58/EC on privacy and electronic communications (e-Privacy Directive). 00350/09/EN, WP 159, 10.02.2009, lk 10.
[155] Council of the European Union. Common position adopted by the Council on 16 February 2009 with a view to the adoption of a Directive of the European Parliament and of the Council amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on consumer protection cooperation. Interinstitutional File: 2007/0248 (COD). 16497/1/08 REV 1. Brussels, 16.02.2009, lk 57.
[156] European Data Protection Supervisor. Opinion. – OJ C 181, 18.07.2008, lk 9–10.
[157] Information Commissioner's Office (ICO). Guidance on the use of cookies and similar technologies, lk 13–14; Article 29 Data Protection Working Party. Opinion 04/2012, WP 194, lk 2–4.

soovitud veebilehe kasutajale saatmiseks teada kasutaja IP-aadressi[158], mis võimaldab tuvastada kasutaja seadme ja on interneti kontekstis põhimõtteliselt kasutaja seadme aadress[159]. Ilma aadressi teadmata ei ole võimalik sõnumit kohale toimetada, seega kohaldub side edastamise erand. Side edastamiseks e-kirja näitel on vaja töödelda nt osapoolte e-posti aadresse, IP-aadresse, kirja saatmise aega, mahtu, kirja pealkirja (*subject*) ja kirjale lisatud faile[160].

Hädavajalikkuse erand tähendab olukorda, kus ilma teabe salvestamiseta kasutaja soovitud teenus ei töötaks. Kui kasutaja logib sisse oma internetipanka ja vaatab kõigepealt konto väljavõtet, seejärel e-arveid ja väärtpaberite seisu, siis tõenäoliselt asuvad need kõik eraldi veebilehtedel (st kõiki neid andmeid ei kuvata järjest loeteluna internetipanga esilehel). Kui kasutaja internetipanga alamlehtede vahel navigeerib, siis ilma autentimisküpsiste kasutamiseta peaks kasutaja iga veebilehe kuvamisel (sh veebilehe värskendamisel) uuesti teenusesse sisse logima. Ent autentimisküpsised aitavad meeles pidada kasutaja sessiooni internetipanga konkreetse külastuse raames. Seega on antud teenuse kasutamiseks hädavajalik kasutada vajalikke küpsiseid.[161]

Hädavajalikkuse erandi alla ei lähe veebisaidi operaatori jaoks olulised või kasulikud küpsised, nagu analüütikaküpsised, olgu need veebisaidi enda või kolmanda osapoole küpsised, ega funktsionaalsed küpsised, mida kasutatakse nt selleks, et tervitada kasutajat sisselogimise järel nimeliselt[162]. Hädavajalikkust tuleb hinnata mitte veebisaidi operaatori seisukohalt, vaid kasutaja perspektiivist. St et kuigi veebisaidi omaniku jaoks võivad nt turundusküpsised olla tulu teenimiseks vajalikud, ei ole need vajalikud kasutaja jaoks[163]. Kehtiva ePD järgi on turundusküpsiste vajalikkus välistatud seda enam, et 2009. aasta muudatuste käigus eemaldati ePD artikli 5 lg-st 3 võimalus salvestada ilma kasutaja nõusolekuta tema lõppseadmesse teavet, mis side edastamist pelgalt toetab.

Käesolevas peatükis analüüsiti küpsistele ja muudele jälgimistehnoloogiatele kohalduva regulatsiooni kujunemist ja töö kirjutamise ajal kehtivat õigust, sh ePD suhet IKÜM-iga seoses kasutaja lõppseadmesse küpsiste salvestamisega. Teise uurimisküsimuse vastuseks saab öelda, et küpsiste kasutamist (ePD järgi laiemalt teabe salvestamist lõppseadmesse ja juurdepääsu sellele) on EL-i õiguses reguleeritud alates 2002. aastast. Kuni 2009. aastani kehtis küpsiste salvestamisel nn loobumispõhine lähenemine, st kasutajat pidi

[158] European Data Protection Supervisor. Opinion. – OJ C 181, 18.07.2008, lk 9–10.
[159] IP-aadress on internetti ühendatud arvuti või muu seadme identifikaator. E-teatmik *sub vero* IP address. – http://vallaste.ee/ (17.04.2021).
[160] Article 29 Data Protection Working Party. Privacy on the Internet, lk 33.
[161] Article 29 Data Protection Working Party. Opinion 04/2012, WP 194, lk 6–7.
[162] Information Commissioner's Office (ICO). Guidance on the use of cookies and similar technologies, lk 14–15.
[163] Information Commissioner's Office (ICO). Guidance on the use of cookies and similar technologies, lk 14.

küpsiste salvestamisest teavitama ning pakkuma talle võimalust küpsistest keelduda. 2009. aastal vastu võetud ePD muudatustega asendati senine loobumispõhine lähenemine eelneva teadliku nõusoleku nõudega. Kehtiva õiguse järgi peab küpsiste salvestamiseks ja muul viisil jälgimiseks antav nõusolek vastama IKÜM-is sätestatud nõuetele, sh olema antud aktiivse tegevusega. Samas ei ole ePD artikli 5 lõikes 3 2009. aastal tehtud põhimõttelist muudatust kõigis liikmesriikides rakendama hakatud, mis on viinud ePD ebaühtlase kohaldamiseni. Järgmises peatükis analüüsitakse kehtivas ePD-s tuvastatud küpsiste ja muude jälgimistehnoloogiate regulatsiooni puuduste parandamiseks uue ePM-i menetlemise käigus välja pakutud lahendusi.

3 Küpsiste (*cookies*) ja muude jälgimistehnoloogiate reguleerimise probleemkohad menetluses oleva e-privaatsuse määruse järgi

3.1 E-privaatsuse määruse menetlemise hetkeseis

Käesoleva töö kirjutamise ajal on uus e-privaatsuse määrus komisjoni, parlamendi ja nõukogu seadusandlikus tavamenetluses (end kaasotsustusmenetlus)[164], mis on peamine seadusandlike aktide vastuvõtmise viis EL-is[165]. Praktikas menetletakse määrusi, direktiive ja otsuseid komisjoni ettepanekute kohta sageli kolmepoolsetel läbirääkimistel (*trilogue*), mis võivad toimuda mistahes seadusandliku tavamenetluse etapis. Kolmepoolsete läbirääkimiste eesmärk on jõuda menetluse võimalikult varajases etapis ühisele seisukohale. Uue ePM-i menetlemisel[166] on valitud just kolmepoolsete läbirääkimiste tee, mis siiski menetlust kiirendanud ei ole. Käesoleva töö kirjutamise ajaks on kõik kolm institutsiooni kujundanud oma seisukoha, mille pinnalt alustada kolmepoolseid läbirääkimisi. Komisjon esitas ettepaneku uue ePM-i vastuvõtmiseks 2017. aastal, parlament võttis oma seisukoha vastu samuti 2017. aastal. Nõukogu arutas ettepanekut umbes neli aastat ning 10. veebruaril 2021 jõudsid liikmesriigid ühise seisukohani. Nõukogu pakub määruse kohalduma hakkamise kuupäevaks 01.08.2022, kuid see sõltub läbirääkimiste käigust.

E-privaatsuse regulatsiooni muutmise vajadus tuleneb eeskätt üldisest EL-i andmekaitsereformist ning täpsemalt vajadusest saavutada kooskõla 2016. aastal vastu võetud IKÜM-iga[167]. Aruandes 2009. aastal muudetud ePD efektiivsuse kohta hindas komisjon direktiivi eesmärke ja põhimõtteid endiselt asjakohaseiks, kuid tõdes, et paljud selle sätted ei täida enam neid eesmärke tehnoloogia ja turu arengute tõttu. Peamiste põhjustena toodi aruandes välja uute side edastamise tehnoloogiate väljajäämine ePD kohaldamisalast, mis on käesoleva töö kirjutamise ajaks lahendatud elektroonilise side direktiivi vastuvõtmisega, ning lõppseadme kaitse tagamiseks rakendatud nõusoleku nõude ebatõhusus, et mitte öelda läbikukkumine. Lisaks on ePD eesmärkide täitmisele mõju avaldanud erinevused liikmesriikide õigustes tulenevalt neile antud diskretsioonist direktiivi ülevõtmisel, ning kohati nõrk

[164] Legislative Observatory. Procedure file 2017/0003(COD). Respect for private life and the protection of personal data in electronic communications. – https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2017/0003(COD)&l=en (26.03.2021).
[165] Euroopa Liidu lepingu konsolideeritud versioon. – ELT C 326, 26.10.2012, lk 13–390, art 294; Craig, P., de Búrca, G. EU Law. Text, Cases, and Materials. Sixth ed. UK: Oxford University Press 2015, lk 124–132.
[166] Menetluse nr 2017/0003(COD).
[167] Nt sisaldab ePD osaliselt IKÜM-iga kattuvaid sätteid, nt andmete turvalisuse (ePD art 4, IKÜM art 32), sätete jõustamise ja järelevalve (ePD art 15, IKÜM IV ptk) ja sanktsioonide kohta (ePD art 15a, IKÜM VIII ptk).

järelevalve ja jõustamine.[168] Regulatsiooni uuendamisega loodetakse luua senisest enam usaldust uute tehnoloogiate ja võimaluste kasutuselevõtu suhtes digiühiskonnas ja -majanduses, millel oleks positiivne mõju ka reklaamitööstuse pakutavate teenuste kontekstis[169].

Küpsiste ja muude jälgimistehnoloogiatega seoses on olulised uue ePM-i lõppseadme kaitset puudutavad sätted, sest küpsiseid salvestatakse kasutaja lõppseadmesse. Samuti on lõppseadmega seotud paljud muud jälgimistehnoloogiad, nagu seadme sõrmejälje jäädvustamine, utlrahelisignaali abil seadme asukoha tuvastamine, masinatevahelise side abil isikute igapäevaelu helide pealtkuulamine (vt ka ptk 1.2). Nii kehtivas ePD-s kui ka uue ePM-i ettepanekus on küpsiste kasutamise ainus võimalik õiguslik alus nõusolek. Seetõttu on käesolevas peatükis rõhk nõusoleku nõude eelistel ja puudustel, eranditel, mis võimaldavad küpsiseid salvestada ilma nõusolekuta, nõusoleku küsimise erinevatel (tehnilistel) võimalustel ning nende mõjul eri huvirühmadele, eeskätt reklaamitööstuses. Enne nõusoleku küsimise praktiliste lahenduste analüüsimist, peatutakse järgmises alapeatükis veidi teoreetilisemal, ent samas siiski potentsiaalselt suure praktilise mõjuga küsimusel, kas nõusolek kui õiguslik instituut on küpsiste kasutuse reguleerimiseks üldse kohane vahend.

3.2 Nõusoleku sobivus küpsiste ja muude jälgimistehnoloogiate kasutamise reguleerimiseks

Nõusoleku eesmärk on tugevdada kasutaja positsiooni ja anda talle otsustusõigus endaga seotud asjaolude üle[170]. 2009. aastal vastu võetud ePD täiendus astus loobumispõhiselt nõustumispõhisele lähenemisele üle minnes küpsiste kasutamise reguleerimisel küll suure sammu edasi, kuid see pole olnud piisavalt efektiivne[171]. Põhjuseid, miks ePD artikli 5 lg 3 ei ole andnud kasutajatele loodetud kaitset, on mitmeid. Esiteks on liikmesriigid nõusoleku nõuet erinevalt kohaldanud ja jõustanud (vt ka 13 liikmesriigi seisukohta art 5 lg 3 muudatuse suhtes ptk 2.3). Teiseks tingis see reegel veebikeskkonnas tõelise küpsisetaotluste laviini, millele kasutaja tüdimuseni reageerima peab ja mis häirivad veebis surfamise kogemust (nim ka

[168] European Commission. Executive Summary of the Ex-post REFIT evaluation of the ePrivacy Directive Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on the protection of privacy and confidentiality in relation to electronic communications and repealing Directive 2002/58/EC („the ePrivacy Regulation"). SWD(2017) 6 final. Brussels, 10.01.2017, lk 2–3.
[169] European Commission. Impact Assessment accompanying the document Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications). SWD(2017) 3 final. Part 2/3. Brussels, 10.01.2017, lk 9; Specht, Kerber, lk 144; Mozilla position paper on the European Commission's draft e-Privacy Regulation. 2017. – https://blog.mozilla.org/netpolicy/files/2017/10/ePrivacy-position-paper-_-FINAL.pdf (23.04.2021), 2–3.
[170] Jones, M. L., Lee, J. Comparing Consent to Cookies: A Case for Protecting Non-Use. – Cornell International Law Journal, Vol. 53, No. 1, 2020, lk 124–125; Solove, D. J. Introduction: Privacy Self-Management and the Consent Dilemma. – Harvard Law Review, Vol. 126, No. 7, 2013, lk 1880.
[171] European Commission. SWD(2017) 6 final, lk 3.

consent fatigue). Kolmandaks ei mõista keskmine IT-hariduseta kasutaja küpsiste kasutamise tagajärgi ehk seda, millega ta tegelikult nõustub, isegi kui talle enne nõustumist kogu nõuetekohane teave esitataks[172].

Õiguskirjanduses on arutletud selle üle, kas nõusolek on üldse sobiv vahend küpsiste kasutamise reguleerimiseks. Solove[173] arutleb nõusoleku dilemma üle, mis seisneb selles, et ühelt poolt tuleb isikule anda kontroll ja õigus otsustada oma isikuandmete kasutuse üle, teiselt poolt on tal seda õigust väga keeruline tõeliselt teostada. Sotsiaalteaduslikud uuringud on näidanud, et inimesed ei suuda alati teha teadlikke ja ratsionaalseid valikuid. Isegi kui nad seda suudaksid, võib oma õiguste kaitsmine käia praktikas üksikisikule üle jõu andmetöötluses osalevate osapoolte arvu ja süsteemi keerukuse tõttu. Teisalt püüdes neid probleeme regulatsiooni tasandil lahendada, võib riik asuda paternalistlikult tegema valikuid inimese eest, mis teistpidi vähendab isiku otsustusõigust ja kontrolli.

See on mh olnud reklaamitööstuse üks paljudest vastuväidetest kasutajate privaatsusõiguste aktiivsele reguleerimisele ja nõusoleku tähtsustamisele, kuid Hoofnagle jt viitavad sellega seoses vaimukalt Tacituse annaalidele, milles kõlavad Cremutius Corduse sõnad: kui sa paned midagi pahaks, siis paistab, et sa tunned selle ära. Hoofnagle jt väidavad – käesoleva töö autori arvates veenvalt –, et paternalistlik on hoopis reklaamitööstuse lähenemine, mis eeldab, et inimesed ei suuda ise teha valikuid toodete-teenuste osas, mis neile huvi pakuvad, ning surub kasutajatele peale käitumispõhist reklaami[174].

Solove püüab nõusoleku dilemmat lahendada argumenteerides, et privaatsuse kaitsmine nõusoleku ja enesejuhtimise (*privacy self-management*) kaudu on endiselt vajalik, kuid leiab, et n-ö paternalistlikult peaks reguleerima vaid isikule äärmiselt kahjulikke juhtumeid ning jätma vähemprobleemsetes küsimustes igaühele vaba otsustusõiguse.[175] Solovega vastupidisel seisukohal on Tene ja Polonetsky[176], kelle arvates on oma õiguste kaitsmise kasutaja kanda jätmine olukorras, kus isegi valdkonna asjatundjad ei suuda selgitada kõiki andmetöötlemise mehhanisme – mis polegi masinõppe ja tehisintellekti kontekstis sageli võimalik[177] –, võrreldav olukorraga, kus raviotsuste langetamine jäetakse patsiendi, mitte arsti hooleks. Käesoleva töö autor nõustub Solovega selles, et teatud baaskaitse peaks isikule olema tagatud, kuid leiab, et nn vaba otsustusõiguse teostamisel on oluline lähtepunkt, millelt seda tegema asutakse. Otsustada on võimalik vabalt nii küpsistest loobudes (*opt out*) kui ka küpsistega nõustudes

[172] European Commission. SWD(2017) 6 final, lk 3.
[173] Solove, lk 1880–1882, 1897, 1903.
[174] Hoofnagle jt, lk 290–291, 294.
[175] Solove, lk 1880–1882, 1897, 1903.
[176] Tene, O., Polonetsky, J. To Track or "Do Not Track": Advancing Transparency and Individual Control in Online Behavioral Advertising. Minnesota Journal of Law, Science & Technology, Vol. 13, No. 1, 2012, lk 285.
[177] Information Commissioner's Office (ICO). Big data, artificial intelligence, machine learning and data protection. Version 2.2. UK: ICO, 2017, lk 9–11.

(*opt in*). See, milliseks kujunevad vaikeseaded, on määrava tähtsusega nii andmekaitse kui ka reklaamitööstuse jaoks[178] (vt ka ptk 3.3).

Nõusoleku kõrval on arutatud küpsiste kasutamisel ka õigustatud huvile tuginemist, nagu see on võimalik IKÜM-i järgi, milles sätestatakse isikuandmete töötlemiseks kokku kuus õiguslikku alust[179]. IKÜM-i kohaselt võib õigustatud huvile tugineda juhul, kui vastutaval töötlejal või kolmandal isikul esineb töötlemiseks õigustatud huvi, isikuandmete töötlemine on selle huvi kaitsmiseks vajalik, ning andmetöötleja huvid kaaluvad üles andmesubjekti huvid või põhiõigused ja -vabadused, kusjuures andmesubjektil on õigus esitada sellisele töötlemisele vastuväide.[180] Õigustatud huvi kui töötlemise aluse roll IKÜM-is on tagada vastutavale töötlejale paindlikkus juhtudel, kus andmesubjektile ei avaldata põhjendamatut mõju, ja muud alused, nagu nõusolek või lepingu täitmise vajadus, ei ole kohased[181].

Õigustatud huvile sooviksid küpsiste kasutamisel tugineda paljud huvirühmad, nagu reklaamitööstus ja sellest sõltuv meedia, telekommunikatsiooniettevõtted, tööstus- ja kaubandussektor ning digimajandus üldisemalt[182]. Globaalselt enam kui 650 meedia- ja tehnoloogiaettevõtet ning kaubamärki ühendav organisatsioon Interactive Advertising Bureau (IAB) argumenteerib, et õigustatud huvile tuginemine peaks olema lubatud, sest see aitaks saavutada suurema kooskõla IKÜM-iga, mh säilitada IKÜM-is vaevaliselt saavutatud kompromisse, ning kuna hiljuti kohalduma hakanud IKÜM juba niigi tagab isikute õiguste tugevama kaitse võrreldes sellele eelnenud andmekaitsedirektiivi ja töö kirjutamise ajal kehtiva ePD-ga[183].

Ootuspäraselt sooviksid õigustatud huvile tuginemist välistada andmekaitseorganisatsioonid[184]. Artikli 29 andmekaitse töörühm on rõhutanud, et õigustatud huvist ei või kujuneda „[tagauks] kõikide selliste andmetöötlustoimingute seadustamiseks, mis ei vasta ühelegi teisele õiguslikule alusele"[185]. Isegi kui EL-i seadusandja otsustab uues ePM-is küpsiste kasutamisel õigustatud huvile tuginemist lubada, leiavad artikli 29 andmekaitse töörühm ja Euroopa Andmekaitsenõukogu, et isikute jälgimist veebisaitide, seadmete, asukohtade ja teenuste üleselt turunduse ja reklaami eesmärgil on raske õigustada

[178] Specht, Kerber, lk 147–148.
[179] IKÜM art 6 lg 1 p a–f.
[180] IKÜM art 6 lg 1 p a ja f, art 21 lg 1.
[181] Article 29 Data Protection Working Party. Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC. 844/14/EN, WP 217, 09.04.2014, lk 10.
[182] Specht, Kerber, lk 133–140; IAB Europe. Interactive Advertising Bureau Europe (IAB). Position, lk 3, 6.
[183] Interactive Advertising Bureau Europe (IAB). Position, lk 2–3.
[184] Specht, Kerber, lk 133–135.
[185] Article 29 Data Protection Working Party. Opinion 06/2014, WP 217, lk 10, 48–49, 51.

andmetöötleja õigustatud huviga[186]. St et praktikas võib õigustatud huvi kui küpsiste kasutamise alus olla reklaamitööstuse osapoolte jaoks kaheldava väärtusega.

Ka komisjoni 2017. aasta ettepanekule esitatud eri huvirühmade seisukohti analüüsinud Specht ja Kerber peavad üllatavaks, et enamik digimajanduse osalisi eelistab IKÜM-i üldiseid reegleid enda arusaama järgi ePD rangematele reeglitele olukorras, kus tegelikult ei ole teada, kuidas täpselt andmetöötlejate õigustatud huve reklaami kontekstis sisustama hakatakse[187]. Kuigi Euroopa Liidu Kohus on andnud suuniseid, kuidas õigustatud huvi olemasolu ja kaalukust Facebookile isikuandmeid edastada võimaldava veebisaidi puhul hinnata[188], on kirjanduses leitud, et interneti kaudu ulatuslikku andmekogumist hõlmavate kaasuste puhul võib töötlemise proportsionaalsusele toetumine kujuneda liiga riskantseks, arvestades liikmesriikide andmekaitseasutuste senist praktikat[189]. Kokkuvõttes võib iseenesest vajaliku paindliku sõnastusega kaasneda sätte prognoosimatu kohaldamine, mis vähendab õiguskindlust kõigi osapoolte jaoks.

Tulles menetluses oleva ePM-i juurde, siis nõukogu on õigustatud huvile tuginemist oma seisukoha kujundamise käigus arutanud[190], kuid kolmepoolsete läbirääkimiste aluseks olevates EK, EP ja EN seisukohtades õigustatud huvi töötlemise alusena ette nähtud ei ole. Selle põhjuseks võib olla asjaolu, et paindlikkust püütakse pakkuda pigem nõusoleku erandite kaudu (vt ka ptk 3.4). Reklaamitööstuse osapooli nõusoleku nõudest erandite sätestamine siiski ei rahulda. Nad argumenteerivad, et EL-i seadusandjal on võimatu ette näha erandit kõigi tekkida võivate olukordade lahendamiseks[191].

Kokkuvõtvalt leiavad Markou ja paljud teised autorid, et vaatamata nõusoleku puudustele, eriti *online*-keskkonnas, on isiku eraelu puutumatuse kaitse tema teadliku nõusolekuga olemuslikult läbipõimunud ning nõusolekut ei saa selles küsimuses ilmselt kunagi päris kõrvale jätta. Markou juhtis 2016. aastal mõnevõrra ootamatult, ent läbinägelikult tähelepanu tõsiasjale, et kuna suured *online*-ettevõtted ei ole pärast 2009. aastat küpsiste kasutamisele kehtima hakanud eelneva nõusoleku nõuet tegelikult järjekindlalt rakendanud, puuduvad piisavad tõendid väitmaks, et nõusoleku nõue küpsiste puhul üldse ei toimi.[192] Seda,

[186] European Data Protection Board (EDPB). Guidelines 8/2020, lk 16; Article 29 Data Protection Working Party. Opinion 06/2014, WP 217, lk 32, 46–47.
[187] Specht, Kerber, lk 143.
[188] EKo C-40/17, *Fashion ID GmbH & Co. KG* versus *Verbraucherzentrale NRW eV*, ECLI:EU:C:2019:629, p 95.
[189] Zuiderveen Borgesius. Personal data processing for behavioural targeting, lk 168.
[190] Council of the European Union. Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications). Interinstitutional File: 2017/0003(COD). 6543/20. Brussels, 06.03.2020, lk 33–35.
[191] Interactive Advertising Bureau Europe (IAB). Position, lk 4.
[192] Markou, C. Behavioural Advertising and the New "EU Cookie Law" as a Victim of Business Resistance and a Lack of Official Determination. – Gutwirth, S., Leenes, R., De Hert, P. (eds). Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection. Netherlands: Springer, 2016. Viidatud siin: From, lk 65.

et veebisaidid on ePD-d tõlgendanud ja kohaldanud väga erinevalt – veebis kohtab nii nõusolekutaotluse puudumist, võimalust töötlemisega üksnes nõustuda, kui ka võimalust lubada valikuliselt teatud liiki töötlemist –, on õiguskirjanduses välja toonud teisedki. On väidetud, et kui jõustataks kehtivaidki reegleid, oleks olukord parem, mis ei tähenda siiski, et regulatsiooni pole tarvis muuta[193]. Niisiis on vaatamata õigusteaduslikule debatile kasutaja nõusolek, teadlikkus ja kontroll jäänud nii EL-i kui ka USA andmekaitseõiguses kesksele kohale[194]. Järgnevalt vaadeldakse uues ePM-is välja pakutud, kuid seni praktikas proovimata lahendust anda nõusolek rakenduse seadete kaudu, mille eesmärk on vähendada kasutajale esitatavate nõusolekutaotluste arvu ja ilma kasutaja loata tema veebitegevuse jälgimist.

3.3 Küpsiste ja muude jälgimistehnoloogiate kasutamiseks nõusoleku andmine rakenduse seadete kaudu

Menetletava ePM-i üks vaieldavamaid küsimusi on küpsiste ja muude jälgimistehnoloogiate kasutamiseks nõusoleku küsimine rakenduse (nt veebilehitseja, operatsioonisüsteemi) seadete kaudu. Samas on see idee põhimõtteliselt sama vana kui küpsised ise. Nimelt soovisid 1997. aastal esimese küpsiste tehnilise standardi[195] autorid keelata veebilehitsejal kolmanda osapoole küpsiste vastuvõtmise või alternatiivselt lubada veebilehitsejal need vastu võtta vaid kasutaja hallatavate seadete kaudu, mis on vaikimisi seadistatud kolmanda osapoole küpsiseid mitte lubama. Erinevatel tehnilistel ja poliitilistel põhjustel ning reklaamitööstuse intensiivse lobitöö tagajärjel jäid kolmanda osapoole küpsised veebilehitsejates siiski lubatuks[196], seega ei järgnenud sellele ideele ei USA ega Euroopa jurisdiktsioonides arutelu veebilehitseja kaudu nõusoleku andmise õiguslike aspektide üle. See diskussioon on aga tekkinud nüüd, 20 aastat hiljem, sest komisjoni 2017. aastal esitatud uue ePM-i ettepanekus on veebilehitseja seadete kaudu nõusoleku andmise võimalus ette nähtud.

Mõlemad senised e-privaatsuse direktiivid[197] on toetunud andmekaitsedirektiivi ja sellele järgnenud IKÜM-i nõusoleku määratlusele, mille artikli 4 p 11 järgi on nõusolek andmesubjekti „vabatahtlik, konkreetne, teadlik ja ühemõtteline tahteavaldus" ning täiendavad nõuded tulenevad artiklist 7. IKÜM-i preambulis selgitatakse, et „nõusolek võiks hõlmata vajaliku lahtri märgistamist veebisaidil, infoühiskonna teenuste tehniliste seadmete valimist või muud avaldust või käitumist, millest selles kontekstis konkreetselt nähtub andmesubjekti

[193] Article 29 Data Protection Working Party. The Future of Privacy. Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data. 02356/09/EN, WP 168, 01.12.2009, lk 2; Hogan & Hartson LLP, lk 291.
[194] Jones, Lee, lk 132.
[195] IETF (Internet Engineering Task Force). HTTP State Management Mechanism. RFC 2109.
[196] Kristol, lk 159–160, 163, 166.
[197] Direktiivi 97/66/EC ja direktiivi 2002/58/EÜ art 2.

nõusolek teda puudutavate isikuandmete kavandatavaks töötlemiseks" (pp 32). Ka 2009. aasta muudatuste direktiivi preambulis mainitakse, et „[k]ui see on tehniliselt võimalik ja tulemuslik vastavalt direktiivi 95/46/EÜ asjakohastele sätetele, võib kasutaja nõusolek andmete töötlemisega väljenduda kohaste brauseri vm rakenduse seadete kasutamises" (pp 66).

Esmapilgul võib jääda mulje, et neis põhjenduspunktides räägitakse samast asjast: nõusoleku andmisest tehniliste seadete kaudu, kuid lähemal vaatlemisel selgub, et tsiteeritud põhjenduspunktid selgitavad kaht täiesti erinevat olukorda. IKÜM-i pp-is 32 käsitletakse lahtri märgistamist või seadete valimist konkreetsel veebisaidil või konkreetse infoühiskonna teenuse seadetes ehk mõeldud on valiku tegemist kindlaksmääratud olukorras ja kontekstis, mitte veebilehitseja või muu rakenduse seadetes üldiselt. Seega selgitab IKÜM-i pp 32 nõusoleku andmist isikuandmete töötlemiseks teatud konkreetsel eesmärgil ja sellisele nõusolekule kehtivad ka kõik muud IKÜM-i nõuded, eeskätt artikli 4 p 11 ja artikkel 7.

Ent 2009. aasta direktiivi pp 66 tervikuna käsitleb küpsiste ja muu teabe salvestamist lõppseadmesse ning räägib nõusoleku andmisest teabe salvestamiseks ja sellele juurdepääsemiseks just nimelt veebilehitseja või muu rakenduse seadete kaudu. Sellise nõusoleku näol on tegemist üldise, kõiki järgnevaid töötlemistoiminguid hõlmava nn generaal- ehk üldnõusolekuga, mis ei saa olla vabatahtlik, konkreetne ega teadlik tahteavaldus. Kui veebilehitseja küsib kasutaja nõusolekut kõikide järgnevate töötlemise eesmärkide suhtes korraga, siis ei ole see vabatahtlik, kuna vabatahtlikkus eeldab võimalust nõustuda iga üksiku eesmärgiga eraldi. Samuti ei saa selline nõusolek olla teadlik ega konkreetne, kuna nõusolek antakse etteulatuvalt nõustumise hetkel veel määratlemata või väga üldsõnaliste eesmärkide suhtes.[198] Samal ajal peab veebilehitseja seadete kaudu antav nõusolek pp-i 66 kohaselt vastama direktiivi 95/46/EÜ asjakohastele sätetele. Kuidas seda tingimust mõista ja täita? Artikli 29 andmekaitse töörühm selgitas 2010. aastal, et selleks et veebilehitseja seadetes antud nõusolek vastaks andmekaitsedirektiivi nõutele, peab rakendus vaikimisi olema seadistatud kolmanda osapoole küpsiseid keelama (vastasel korral ei ole nõusolek töötlemisele eelnev ega konkreetne) ning kasutajale tuleb esitada selge, täielik ja hästi nähtav teave küpsiste kasutamise eesmärkide kohta, sh viited reklaamivõrgustikele, kes on küpsise salvestajaks ja kelle nimel teavet esitatakse (et nõusolek oleks teadlik). Artikli 29 andmekaitse töörühm leidis 2010. aastal, et selliseid juhte esineb väga piiratult, mh seetõttu, et tol hetkel neljast suurimast veebilehitsejast ainult üks keelas küpsiste salvestamise vaikimisi.[199]

[198] Article 29 Data Protection Working Party. Opinion 2/2010 on online behavioural advertising, lk 14; European Data Protection Board (EDPB). Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1. 04.05.2020, lk 12–15.
[199] Article 29 Data Protection Working Party. Opinion 2/2010 on online behavioural advertising, lk 13–15.

Huvitav on küsimus, miks ei järgnenud 2009. aasta muudatustele veebilehitseja seadete kaudu antava nõusoleku tingimuste ja kehtivuse üle kuigi tõsist arutelu. Esiteks võib põhjus olla selles, et põhjenduspunktil on erinevalt artiklist selgitav, mitte siduv iseloom. Artikli 29 andmekaitse töörühm selgitas 2010. aastal, et ePD pp 66 ei ole erand artikli 5 lg-st 3, vaid meeldetuletus, et tänapäeva tehnoloogilises keskkonnas on nõusolekut võimalik anda mitmel viisil (eeldusel, et see viis vastab direktiivi 95/46/EÜ asjakohastele sätetele)[200]. Teiseks, nagu viidati käesoleva töö peatükis 2.3, oli 13 liikmesriigil 22-st vastuoluline arusaam, et kuigi 2009. aasta direktiivi artikli 5 lg 3 sätestab nõusoleku nõude enne kasutaja lõppseadmesse teabe salvestamist, ei muuda see siiski olemasolevat reeglit, et nõusolekut võib väljendada kasutaja teavitamise ja talle loobumisvõimaluse pakkumisega[201]. Seega pole üllatav, et ePD tõhususe hinnangutes[202] on korduvalt esile toodud liikmesriikide erinevat praktikat ePD ülevõtmisel üldises plaanis ja eriti artikli 5 lg 3 muudatuse rakendamisel. Bond[203] nendib 2012. aastal, et kuigi 2009. aasta direktiiv pidi olema liikmesriikide õigustesse üle võetud 25. maiks 2011 (2009. aasta direktiivi art 4), ei olnud 4 liikmesriiki seda veel teinud ja ülejäänud 18 seas oli neid, kes otsustasid, et olemasolevat õigust ei ole direktiivi ülevõtmiseks tarvis muuta. Eelnevat arvestades sedastas Bond, et veebilehitseja kaudu nõusoleku taotlemine on alles tööjärgus olev idee, kuigi paljud liikmesriigid nägid seda lahendusena nõusoleku probleemidele[204].

Igal juhul on võrreldes 2009. aasta direktiiviga uues ePM-is rakenduse kaudu nõusoleku küsimine esiteks toodud määruse põhiteksti ja teiseks on see sõnastatud selgemalt. Nimelt on uues ePM-is nõusoleku kohta ette nähtud eraldi artikkel[205], mille lõikes 1 sätestatakse, et üldjuhul kohaldatakse nõusolekule IKÜM-i artikli 4 p 11 ja artiklit 7, ning lõikes 2 lisatakse, et lõppseadme kaitse kontekstis võib nõusolekut väljendada rakenduse seadete kaudu, kui see on tehniliselt võimalik ja teostatav. Nende kahe lõike koosmõjus peab nõusolek olema „vabatahtlik, konkreetne, teadlik ja ühemõtteline tahteavaldus", kuid lõppseadme kaitse kontekstis kehtib lisareegel, mille järgi võib nõusoleku anda ka rakenduse seadete kaudu. Muudel juhtudel, nt sisu- või metaandmete töötlemiseks[206] antav nõusolek peab endiselt vastama kõigile IKÜM-i nõuetele. See lahendus ei ole probleemivaba, sest lisareeglile vaatamata jääb sisuline probleem alles: kõikehõlmav üldnõusolek on vastuolus IKÜM-i nõuetega.

[200] Article 29 Data Protection Working Party. Opinion 2/2010 on online behavioural advertising, lk 13–15.
[201] Council of the European Union. 15864/09 ADD 1 REV 1, lk 3.
[202] Nt Deloitte, lk 87–88.
[203] Bond, R. The EU E-Privacy Directive and Consent to Cookies. – Business Lawyer (American Bar Association), Vol. 68, No. 1, 2012, 215–217.
[204] Bond, lk 216.
[205] EK ja EP seisukohtade art 9; EN seisukoha art 4a.
[206] Kõigis seisukohtades ePM art 6.

Lõppkokkuvõttes on nõusoleku küsimine veebilehitseja seadete kaudu siiski EL-i seadusandja silmis õiguslikult pädev. Seda seisukohta toetab ka käesoleva töö autor, sest põhimõtteliselt ei ole keelatud võtta ühe õigusakti sätteid teise õigusakti üle ja neid vastavalt teise õigusakti vajadustele kohandada. Et nii EK, EP kui ka EN seisukohad lubavad anda küpsiste kasutamiseks nõusoleku rakenduse seadete kaudu, võib eeldada, et see küsimus on põhimõtteliselt otsustatud. Ent milles ei ole üksmeelt ja mis on praktikas tõelise muutuse esilekutsumisel määrava tähtsusega, on EL-i seadusandja otsus, millised saavad olema rakenduse vaikimisi seaded ehk kasutaja lähtepositsioon enda valikuvabaduse teostamisel. Järgnevalt analüüsitakse, miks on lõimitud ja vaikimisi andmekaitse isiku privaatsusõiguste tagamisel olulised, millistel seisukohtadel on selles osas EK, EP ja EN ning kuidas võivad EL-i seadusandja valikud mõjutada eri huvirühmade tegevust tulevikus.

IKÜM-i artiklist 25 tulenevad vaikimisi ja lõimitud andmekaitse põhimõtted kohalduvad kehtivale ePD-le ja uuele ePM-ile üldviite[207] kaudu, mille kohaselt ePM täiendab ja täpsustab IKÜM-i sätteid elektroonilise side valdkonnas. Lõimitud andmekaitse tähendab töötlemisvahendite kindlaksmääramisel ja isikuandmete töötlemise ajal asjakohaste tehniliste ja korralduslike meetmete kasutamist, mis on vajalikud andmekaitsepõhimõtete (IKÜM II ptk, eriti art 5) tõhusaks rakendamiseks (IKÜM art 25 lg 1). Selleks võivad olla mitmesugused meetmed alates kõrgtehnoloogilistest lahendustest kuni töötajatele mõeldud küberhügieeni teemaliste koolitusteni[208]. Üheks konkreetseks näiteks tehnoloogia tasandil lõimitud andmekaitsest on otspunktkrüpteerimine[209] (*end-to-end encryption*), mis peaks Euroopa Andmekaitsenõukogu hinnangul olema side valdkonnas üldreegel[210], aga täna seda ei ole. Vaikimisi andmekaitse tähendab asjakohaste tehniliste ja korralduslike meetmete rakendamist, millega tagatakse, et vaikimisi töödeldakse ainult selliseid isikuandmeid, mis on vajalikud töötlemise konkreetse eesmärgi saavutamiseks (IKÜM art 25 lg 2). Küpsiste näitel tähendab lõimitud andmekaitse seda, et rakenduses peab olema tehniliselt võimalik küpsiste salvestamisest keelduda. Vaikimisi andmekaitse tähendab, et enne rakenduse kasutama asumist peab kaitse n-ö olema sisse lülitatud ehk küpsiste salvestamine keelatud.

Lõimitud andmekaitse on oluline, sest see võimaldab n-ö alustada ahela algusest. Raadiosagedustuvastuse (RFID) puhul rõhutas artikli 29 andmekaitse töörühm 2005. aastal, et kuigi RFID-i tehnoloogia rakendajad vastutavad isikuandmete eest, mida nad selle abil

[207] ePD art 1 lg 2; ePM-i kõigis seisukohtades art 1 lg 3.
[208] European Data Protection Board (EDPB). Guidelines 4/2019 on Article 25 Data Protection by Design and by Default. Version 2.0. 20.10.2020, lk 6.
[209] Otspunktkrüpteerimise korral andmed krüpteeritakse lähtepunktis ja dekrüpteeritakse sihtpunktis, st teekonna vältel on andmed krüpteeritud. Corrigan.
[210] Article 29 Data Protection Working Party. Opinion 03/2016 on the evaluation and review of the ePrivacy Directive, lk 19; European Data Protection Board (EDPB). Statement 03/2021 on the ePrivacy Regulation, lk 2.

koguvad, lasub vastutus ka RFID-iks kasutatavate vahendite ja seadmete tootjatel ja standardiorganisatsioonidel, tagamaks isiku eraelu puutumatust kaitsvate seadmete olemasolu turul[211]. Vaikimisi andmekaitse on oluline, sest tavakasutaja ei suuda orienteeruda info- ja kommunikatsiooni valdkonna tehnilistes üksikasjades, et teha teadlikke valikuid[212]. Vaikimisi kaitse aitab vähendada eraelu puutumatuse riivet ja sellest tulenevat kahju, mida võib üksikisikul olla keeruline tuvastada ja vaidluse korral tõendada; see vähendab võimalust, et üksikisik peaks hakkama tegelema küsimusega, millise andmemajanduse ökosüsteemis osaleja poole oma õiguste kaitseks pöörduda; ning kaitseb sarnaselt tarbijaõigusega nõrgemat osapoolt. Lisaks mõjutab inimeste käitumist kalduvus jääda passiivseks (*status quo bias*, *inaction bias*) ehk mitte muuta olemasolevaid seadeid ning kalduvus otsustada käeulatuses oleva olevikuhüve kasuks tulevikutagajärgi kaalumata (*present bias*)[213], kusjuures ulatusliku andmekogumise tagajärgi võib olla väga keeruline ette näha[214]. Vaikimisi kaitse korral töötab vähemalt *status quo* säilitamise kalduvus isiku eraelu puutumatuse kaitseks. Käesoleva töö autor leiab samuti, et kasutaja võiks asuda oma autonoomiat teostama vaikimisi kaitse positsioonilt, millest tal on võimalik konkreetsel juhul omal soovil kõrvale kalduda. St et vabadus valida on tagatud, kuid tegevusetuse korral ei jääks isik kaitseta.

Spechti ja Kerberi koostatud ülevaates komisjoni 2017. aasta ettepanekule reageerinud huvirühmade seisukohtadest nõuavad rakenduse seadetes vaikimisi privaatsuse kaitsmist andmekaitse eestkõnelejad. Nad juhivad tähelepanu nõusoleku senistele probleemidele ning koormale ja kulule, mida kasutaja peab kandma igal üksikul veebisaidil küpsiste keelamiseks[215]. Vaikimisi küpsiste keelamise vastu on selgelt reklaamitööstus ja reklaamitulust sõltuvad veebisaidid, nagu *online*-ajakirjandus. Paljude veebisaitide jaoks on tasuta veebisisu esitamine võimalik vaid tänu veebisaidil oleva vaba reklaamipinna väljaüürimisele. Nagu peatükis 1.3 selgitati, on reklaamipind rohkem väärt nii veebisaidi omanikule kui ka reklaamijale, kui on teada, kes seal kuvatavat reklaami näeb. Kui veebilehitsejad seadistatakse vaikimisi küpsiseid keelama, väheneb isikute kohta saadaolevate andmete maht ja mitmekesisus drastiliselt, mis seab ohtu käitumispõhisele reklaamile rajatud ärimudelid. Reklaamitööstus toob välja, et kui kasutaja langetab otsuse juba veebilehitseja seadetes, võetakse ülejäänud osalistelt, sh kolmandatelt osapooltelt (nt andmevahendajalt, reklaamivõrgustikult) võimalus kasutajaga üldse dialoogi astuda, et temalt küpsise

[211] Article 29 Data Protection Working Party. Working document on data protection issues related to RFID technology, lk 12.
[212] Tene, Polonetsky, lk 285.
[213] Zuiderveen Borgesius. Informed Consent, lk 105; Kristol, lk 164–165; Zuiderveen Borgesius, F. J., Kruikemeier, S. jt. Tracking Walls, Take-It-Or-Leave-It Choices, the GDPR, and the ePrivacy Regulation. – European Data Protection Law Review, Vol. 3, No. 3, 2017, lk 358–359.
[214] Solove, lk 1902.
[215] Specht, Kerber, lk 145, 148.

salvestamiseks nõusolekut küsida. See nõue mõjutaks rohkem väikese külastajate arvuga veebisaite, reklaamivahendajaid ja oma teenuste reklaamijaid, sest suurtel teenuse osutajatel, nagu Google ja Facebook on võimalik luua oma miljonite kasutajatega otsekontakt ja küsida neilt nõusolekut teenusesse sisselogimisel.[216]

Reklaamitööstuse argumente ei saa eirata. On selge, et rakenduse tasemel küpsiste kasutamise keelamine vaikimisi mõjub rängalt paljudele reklaamimajanduse osapooltele. Samas on õiguskirjanduses juhitud tähelepanu sellele, et käitumispõhine reklaam ei ole ainuvõimalik reklaamimise viis. Reklaam iseenesest ja olemuslikult ei eelda isikute jälgimist. Enne käitumispõhise reklaami levikut oli tavapäraseim toodete ja teenuste reklaamimine kontekstipõhiselt ehk autosid reklaamiti autodega seotud veebisaitidel, aiandustooteid koduajakirjades – seda nii veebis kui ka paberväljaannetes.[217] Samuti on tavapärane teatud tunnuste alusel turu segmenteerimine tarbijarühmadesse, mille käigus ei toimu üksikisikute tuvastamist ja iga nende liigutuse jälgimist nagu käitumispõhise reklaami puhul. Sarnaselt arutles juba 2001. aastal Kristol, esimese küpsiste tehnilise standardi üks autoritest: kolmanda osapoole küpsiste vaikimisi keelamine ähvardab reklaamitööstuses levinud *ärimudeleid*, mis rajanevad isikute jälgimisel, kuid mitte reklaamide esitamist veebis põhimõtteliselt ja ammugi mitte reklaamitööstust kui sellist[218]. See eristus on äärmiselt oluline. Ka küpsiseid keelavate rakenduse vaikeseadete korral jääks võimalikuks oma toodete ja teenuste reklaamimine kui selline, sh käitumispõhiselt nendele isikutele, kes on selleks soovi avaldanud. Zuiderveen Borgesiuse jt 2017. aastal läbi viidud küsitluse järgi peavad inimesed tasuta teenuste kasutamisel vastuvõetavamaks seda, et nad peavad nägema reklaame, kui seda, et nende kohta kogutakse andmeid. Seega on inimesed mõistnud ja aktsepteerivad seda, et tasuta sisu maksavad kinni reklaamijad, kuid peavad ebaõiglaseks enda jälgimist reklaami esitamiseks[219].

Äärmiselt huvitav on siinkohal veebilehitseja Firefox omaniku Mozilla Corporation seisukoht[220] komisjoni 2017. aasta ePM-i ettepaneku suhtes, millele Specht ja Kerber oma analüüsis tähelepanu juhivad[221]. Mozilla seisukoht erineb kardinaalselt peaaegu kõigi teiste digimajanduse osapoolte arvamustest, sest Mozilla toetab komisjoni ettepanekut ning püüdleb jätkusuutlikuma mudeli poole, milles kasutaja kontroll, valikud ja läbipaistvus eksisteerivad kõrvuti majanduslikult tasuvate ärimudelitega. Mozilla seisab n-ö ebameeldivate üllatuste vaba internetireklaami eest: kui soovitakse koguda isikuandmeid personaalsete teenuste

[216] Specht, Kerber, lk 136–137.
[217] Zuiderveen Borgesius, Kruikemeier jt, lk 358.
[218] Kristol, lk 160–161, 163.
[219] Zuiderveen Borgesius, Kruikemeier jt, lk 356–358.
[220] Mozilla position paper.
[221] Specht, Kerber, lk 140.

pakkumiseks, siis tuleb seda teha isiku privaatsust austades ja tema nõusolekul[222]. Mozilla seisukoht näitab, et eraelu puutumatuse kaitse ja digimajandus ei pea teineteisele vastanduma. Reklaamitööstus mõistagi suhtub Mozilla nägemusse väga kriitiliselt[223].

EK, EP ja EN seisukohtades vaikimisi ja lõimitud andmekaitse osas üksmeelt käesoleva töö kirjutamise ajal ei ole. Kõige rohkem kaitset pakub kasutajale EP seisukoht, seejärel EK ettepanek ning kõige vähem EN positsioon. EP seisukohas sätestatakse, et vaikimisi peab elektroonilist sidet, sh internetis teabe hankimist ja kuvamist võimaldav turule lastav tarkvara olema seadistatud kolmanda isiku poolt lõppseadmesse teabe salvestamist, selles oleva teabe töötlemist ja selle kohta teabe kogumist keelama[224]. EP seisukohas nähakse ette üksikasjalikud – Mozilla arvates ehk liigagi[225] – reeglid seadete haldamise võimaluse pakkumiseks tarkvara installimisel ja pärast seda ning sätestatakse kasutaja tahteavalduse siduvus ja jõustatavus kolmanda isiku suhtes[226]. Seadete kaudu antavad nõusolekud peaksid olema piisavalt eristatud eri eesmärkide kategooriate tasemel (nt eraldi nõusolekud turunduslikul või veebianalüütika eesmärgil jälgimiseks)[227] (vt ka Joonis 5). Jõustamise seisukohalt on eriti tervitatavad EP seisukoha lõpus olevad sätted, mis panevad teenuse osutajatele ja liikmesriikidele konkreetseid kohustusi[228].

EK seisukoht on lõimitud ja vaikimisi andmekaitse põhimõtete rakendamisel ebajärjekindel[229]. Ühelt poolt viitab EK ettepanek pp-is 23 otsesõnu IKÜM-is sätestatud lõimitud ja vaikimisi andmekaitsele, kuid artikli 10 lg-s 1 sätestab, et „[e]lektroonilist sidet, sealhulgas internetis teabe hankimist ja kuvamist võimaldav turule lastud tarkava *pakub võimalust keelata* kolmandal isikul lõppkasutaja lõppseadmesse teabe salvestamine või juba lõppseadmesse salvestatud teabe töötlemine" (autori rõhutus). Seega lõimitud kaitse põhimõtet järgitakse (küpsiste keelamine on tehniliselt võimalik), kuid vaikimisi kaitse põhimõtet mitte. Võib-olla püütakse seda kompenseerida artikli 10 lg-ga 2, mille kohaselt ei saa kasutaja rakenduse installimist enne jätkata, kui ta on valinud endale sobivad privaatsusseaded. Samas tundub selline kohustamine siiski ülemäärane ja võib pigem kutsuda esile kasutaja pahameele.

---

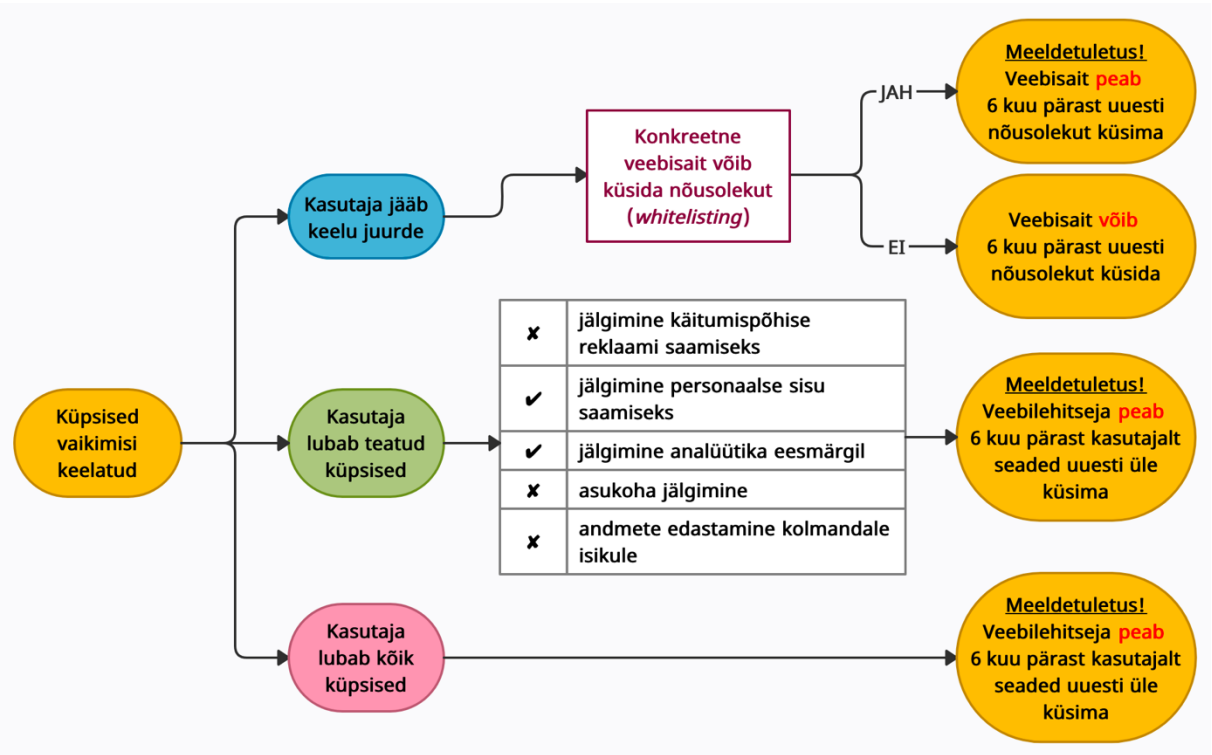
[222] Sullivan, J. Personalization with Respect. (10.05.2013) – https://blog.mozilla.org/blog/2013/05/10/personalization-with-respect/ (22.04.2021).
[223] Rothenberg, R. Has Mozilla Lost its Values? (16.07.2013) – https://www.iab.com/news/has-mozilla-lost-its-values/ (22.04.2021).
[224] EP seisukoha art 10 lg 1 p a.
[225] Mozilla position paper, lk 9–10.
[226] EP seisukoha art 10 lg 1a uus lõik.
[227] EP seisukoha pp 23.
[228] Nt EP seisukoha art 17 lg-te 1a ja 1b järgi ei tohi elektroonilise side ja infoühiskonna teenuste osutajad ning internetis teabe hankimist ja kuvamist võimaldava tarkvara tootjad kasutada mingeid meetmeid, mis võivad takistada kasutajatel rakendada parimaid olemasolevaid vahendeid sissetungi ja viiruste vastu ning nende võrkude, lõppseadmete ja elektroonilise side turvalisuse jaoks. Liikmesriigid ei või kehtestada tarkvara tootjatele kohustusi, mis võiksid nõrgestada nende võrkude ja teenuste või lõppseadmete konfidentsiaalsust ja terviklust, sealhulgas kasutatavaid krüpteerimismeetodeid.
[229] Specht, Kerber, lk 129.

EK ja EP seisukohtades nähakse ette ka üleminekukord: lõppseadmesse juba installitud tarkvara tuleb ePM-iga vastavusse viia kas esimese tarkvarauuenduse ajal või kolme kuu jooksul alates ePM-i vastuvõtmisest[230] või kuue kuu jooksul alates ePM-i jõustumisest[231].

Kahetsusväärselt on arutelude käigus EN seisukohast artikkel 10 sootuks kustutatud ning viidet lõimitud ja vaikimisi andmekaitsele pole ka preambulis. Kuigi lõimitud ja vaikimisi andmekaitse põhimõtted hakkavad üldviite[232] kaudu siiski ePM-ile kohalduma, võivad need ilma siduva artiklita jääda abstraktseks ja praktikasse mitte jõuda.

Kuigi rakenduse seadete sisus ei ole töö kirjutamise ajal EK, EP ja EN seisukohtades konsensust, võib püüda mudeldada, kuidas nõusoleku küsimine välja võiks näha. Peamiselt EK ja EP seisukohtade alusel koostatud Joonis 5 illustreerib küpsiste kasutuse seadistamist veebilehitseja seadetes ja nende kasutamiseks konkreetsel juhul nõusoleku küsimist veebisaidi poolt. Joonisel kajastatakse seda, kuidas veebisaidid saavad siiski luua otsekontakti ehk astuda dialoogi kasutajaga, vaatamata veebilehitseja seadistusele. EP ja EN seisukohad sätestavad selgelt, et konkreetsel veebisaidil antud nõusolek on ülimuslik veebilehitseja seadete suhtes[233] (Joonisel *whitelisting*).

Joonis 5. Näide nõusoleku küsimise kohta veebilehitseja seadete ja hiljem veebisaidi kaudu



Allikas: EK seisukoha art 9 lg 3; EP seisukoha pp 23, art 10 lg 1 p a järgi koostanud magistritöö autor

[230] EK seisukoha art 10 lg 3.
[231] EP seisukoha art 10 lg 3.
[232] ePD art 1 lg 2; ePM art 1 lg 3.
[233] EP seisukoha art 10 lg 1b; EN seisukoha art 4a lg 2aa.

Selline süsteem kaitseks kasutajate eraelu puutumatust vaikimisi, kuid samas ei kahjustaks kasutaja autonoomiat ning võimaldaks konkreetsel veebisaidil saada kasutaja nõusolek ka juhul, kui veebilehitseja on üldiselt seadistatud küpsiseid vaikimisi keelama. See aitaks vähendada negatiivset mõju reklaamitulust sõltuvatele veebisaitidele. Siiski on oht, et tsentraliseeritud lähenemise peamine eelis – nõusolekutaotluste arvu vähendamine – ei kujune nõnda mõjusaks, kui loodetakse, just nimelt konkreetsete veebisaitide nõusolekutaotluste tõttu[234]. Teiseks on oht, et kasutaja koormatakse üle meeldetuletustega. Mozilla leiab, et iga kuue kuu järel kasutaja teavitamine võimalusest loobuda küpsiste kasutamisest on juba piisavalt reguleeritud IKÜM-i artikli 7 lg-s 3, mille järgi tuleb kasutajat enne nõusoleku andmist teavitada võimalusest nõusolek igal ajal tagasi võtta ning võimaldada tal seda teha sama lihtsal viisil, kui ta nõusoleku andis[235]. Eesti Infotehnoloogia ja Telekommunikatsiooni Liit arvab samuti, et iga kuue kuu järel kasutajale meeldetuletuse saatmine oleks tarbetult koormav nii teenuse osutajale kui ka kasutajale ning ei lahendaks praegust kasutajakogemuse häirituse probleemi[236]. Seda on EP seisukohas juba arvesse võetud[237]. Lisaks sätestab EN seisukoha artikli 4a lg 3, et kasutajale peab nõusoleku tagasivõtmist meelde tuletama perioodiliselt, v.a kui kasutaja on avaldanud soovi selliseid meeldetuletusi mitte saada.

Käesoleva töö autor rõhutab, et ülaltoodud joonis näitlikustab vaid üht võimalikku mudelit ja keskendub üksnes küpsistele ja veebikeskkonnale. Nagu eespool öeldud, on rakenduse seadetes vaikimisi kaitse kohaldamine käesoleva töö kirjutamise ajal veel lahtine. Lisaks küpsistele ja veebilehitsejale tuleb arvestada muude seadmete ja tehnoloogiatega, mis on võimelised internetiga ühenduma või muul moel kasutaja tegevust jälgima, st tuleb hõlmata mitte üksnes mobiiltelefonid ja tahvelarvutid, vaid ka nutikellad, tervisemonitorid ja targad kodumasinad[238]. Paljude selliste seadmete puhul võib sobiv ühtne nõusoleku haldamise koht olla operatsioonisüsteemi seaded, mitte iga rakenduse seaded eraldi.

Tehnilisi võimalusi nõusoleku andmiseks rakenduse seadetes on palju. Artikli 29 andmekaitse töörühm[239] soovitab arvamuses ePM-i ettepaneku kohta teha veebilehitsejatele

[234] Interactive Advertising Bureau Europe (IAB). Position, lk 1, 5.
[235] Mozilla position paper, lk 8–9.
[236] Eesti Infotehnoloogia ja Telekommunikatsiooni Liit (ITL). Arvamus Euroopa Komisjoni poolt 10.01.2017. avaldatud e-privaatsuse määruse ettepaneku kohta. Esitatud Majandus- ja Kommunikatsiooniministeeriumile 02.02.2017, lk 4.
[237] EP seisukoha art 9 lg 3.
[238] European Data Protection Board (EDPB). Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications. Version 1.0. 28.01.2020, lk 5; Zanfir-Fortuna, G. Will the ePrivacy Reg overshadow the GDPR in the age of IoT? International Association of Privacy Professionals. (16.02.2017) – https://iapp.org/news/a/will-the-eprivacy-reg-overshadow-the-GDPR-in-the-age-of-iot/ (07.04.2021).
[239] Article 29 Data Protection Working Party. Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC). 17/EN, WP 247, 04.04.2017, lk 17.

kohustuslikuks teatud tehnilise standardi, nagu nt Do Not Track'i[240] rakendamine. Do Not Track'i on arendanud rahvusvaheline standardiorganisatsioon World Wide Web Consortium (W3C)[241], mis töötab välja avatud standardeid interneti ja veebi jaoks ning mida juhib 1989–90. aastatel interneti loonud Tim Berners-Lee. Jones ja Lee[242] annavad üsna põhjaliku ülevaate Do Not Track'i algatusest (2007), vastuseisule allavandumisest (2019) ning mitmest sahtlisse jäänud USA seaduseelnõust, mis oleksid võinud reguleerida küpsiste ja muude jälgimistehnoloogiate kasutust, samuti Euroopa pingutustest küpsiste reguleerimisel, mida on tehtud aastast 2002, kuid – nagu ka käesolevas töös on leitud – siiani edutult. Kantuna ePM-i ettepanekus sätestatavast küpsiste haldamise võimalusest veebilehitseja seadete kaudu ning senaator Ron Wydeni 2018. aastal esitatud seaduseelnõust Consumer Data Protection Act, mis näeks sarnaselt ette kasutajatele ühtse seadete haldamise koha, lõpetavad Jones ja Lee oma artikli lootusrikkalt[243].

Do Not Track ei ole siiski valmis lahendus, sest selle täpses tehnilises sisu ei ole konsensust ja universaalset standardit ei ole tänini õnnestunud luua[244]. Mozilla rõhutab, et kuni ei ole kokkulepitud standardit selle kohta, mida veebisait peab tegema, kui ta saab veebilehitsejalt Do Not Track'i signaali, on seda nõuet – isegi kui sel on juriidiline jõud – raske ellu viia[245]. EP seisukoha pp 22 mainib rakenduse poolt kolmandale osapoolele saadetavat vastavasisulist signaali, kuid mõistlik oleks anda ePM-iga volitused sobivale asutusele, nt komisjonile korraldada Do Not Track'i rakendamiseks tehniliste standardite väljatöötamist (vt ka ptk 3.5). Käesoleva töö autor toetab ühtse tehnilise võimalikult paljude teiste rakendustega ühilduva standardi loomist, mis hõlmaks ka muid jälgimistehnoloogiaid peale küpsiste.

Küpsiste kasutamiseks nõusoleku küsimisega – olgu veebilehitseja seadetes või üksikul veebisaidil – on seotud veel üks reklaamitööstuse jaoks väga oluline küsimus. Õiguskirjanduses on juhitud tähelepanu sellele, et kolmanda osapoole küpsiste keelamisega võivad kaasneda nn jälgimisküpsiste barjäärid (*tracking wall, cookie wall*)[246]. St et kasutajal pole võimalik veebisisuni jõuda, kui ta pole küpsistega nõustunud, mis omakorda tähendab, et paljudel veebisaitidel võidakse küpsiste jaoks üks nõusoleku küsimise hüpikaken lihtsalt asendada teise hüpikaknaga, millel kuvatakse teade stiilis „pole küpsist, pole juurdepääsu"[247]. Seda tehakse

[240] World Wide Web Consortium. Tracking Compliance and Scope. W3C Working Group Note 22 January 2019. – https://www.w3.org/TR/tracking-compliance/ (07.04.2021).
[241] World Wide Web Consortium. – https://www.w3.org/Consortium/ (07.04.2021).
[242] Jones, Lee, lk 97–124.
[243] Jones, Lee, lk 128–129.
[244] Jones, Lee, lk 110.
[245] Mozilla position paper, lk 8.
[246] Zuiderveen Borgesius, Kruikemeier jt, lk 353.
[247] i-SCOOP. The new EU ePrivacy Regulation: what you need to know. (*sine anno*) – https://www.i-scoop.eu/GDPR/eu-eprivacy-regulation/ (28.03.2021).

juba praegu mh seoses reklaamiblokeerijate (*ad blocker*) kasutamisega. Ühest küljest on küpsisebarjääri kasutamine vastuolus IKÜM-i nõusoleku vabatahtlikkusega, mis eeldab, et nõusolek ei ole seatud teenuse osutamise tingimuseks, kui kõnealune töötlemine ei ole vastava teenuse osutamiseks vajalik[248]. Seejuures on kehtiva ePD ja IKÜM-i vahel ebakõla, kuna ePD pp 25 selgelt lubab teha juurdepääsu veebisisule nõusolekust sõltuvaks (vt ka ptk 2.2), millele praktikas ilmselt tuginetaksegi[249]. Teiselt poolt piirab tingimusliku juurdepääsu keelamine veebisaitide ja rakenduse loojate ettevõtlusvabadust, eriti arvestades reklaamitulu olulisust nende tegevuses[250].

Euroopa Andmekaitseinspektor, Euroopa Andmekaitsenõukogu ja artikli 29 andmekaitse töörühm on kindlal seisukohal, et küpsisebarjäärid tuleb keelustada[251]. Samas ei lahenda nad õigustatud küsimust, kas kedagi saab kohustada pakkuma tasuta teenust. Küpsisebarjääri keelamise tõttu võivad teatud teenusepakkujad olla sunnitud tegevuse lõpetama, mille tõttu võib väheneda teenuste mitmekesisus ja konkurents, või jääb juurdepääs veebisisule nn maksumüüri (*pay walls*) taha[252]. See ei pruugi lõppkokkuvõttes olla kasutajate huvides[253].

Üheks kompromissiks võib olla artikli 29 andmekaitse töörühma tõlgendus, mille järgi ePD pp-is 25 sisalduv fraas „juurdepääs *teatavale veebilehe sisule* võib sõltuda küpsise (...) vastuvõtmisest" (autori rõhutus) viitab sellele, et kehtiv ePD lubab kasutada küpsisebarjääre veebisaidi teatud alamlehtede külastamisel, aga mitte piirata juurdepääsu kogu veebisaidile[254]. *Online*-ajakirjanduses tähendaks see tõlgendus seda, et uudisteportaal peab igaühele võimaldama juurdepääsu portaali esilehele, kuid võib nõuda küpsistega nõustumist või tasu teatud artiklite ja arvamuslugude lugemiseks. Täit õiguslikku selgust selles küsimuses siiski ei ole. Euroopa Liidu Kohus märkis 2019. aastal *Planet49* lahendis, et kuna eelotsusetaotluse esitanud kohus ei ole esitanud küsimust selle kohta, kas asjaolu, et kasutaja peab auhinnamängus osalemiseks küpsiste salvestamisega nõustuma, on kooskõlas nõusoleku vabatahtlikkuse nõudega, ei ole kohtul alust seda küsimust käsitleda[255]. Uue ePM-i arutamisel olnuks hea kohtu seisukohta arvesse võtta.

---

[248] IKÜM art 7 lg-s 4 on küll juttu lepingu täitmisest, kuid seda saab analoogia korras üle kanda veebisaidi külastamisele; ka IKÜM pp 43; European Data Protection Board (EDPB). Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1. 04.05.2020, lk 10–12.
[249] Information Commissioner's Office (ICO). Guidance on the use of cookies and similar technologies, lk 30.
[250] Zuiderveen Borgesius, Kruikemeier jt, lk 364.
[251] European Data Protection Supervisor. Opinion 6/2017, lk 16–17; Article 29 Data Protection Working Party. Opinion 03/2016 on the evaluation and review of the ePrivacy Directive, lk 16–17; Article 29 Data Protection Working Party. Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation, lk 15.
[252] Rothenberg; Interactive Advertising Bureau Europe (IAB). Position, lk 4.
[253] Specht, Kerber, lk 147.
[254] Article 29 Data Protection Working Party. Working Document 02/2013, WP 208, lk 5.
[255] C-673/17, *Planet49*, p 64.

EK, EP ja EN seisukohtades käesoleva töö kirjutamise ajal küsimuses, kas küpsistega nõustumine võib olla veebisisule juurdepääsemise tingimus, ühine arusaam puudub. EK seisukoht sisule tingimuslikku juurdepääsu ei käsitle, st järelikult peab EK seisukoht neid lubatavaks. EP seisukohas on see siduva artikliga sõnaselgelt keelatud sõltumata sellest, kas teenust osutatakse raha eest või tasuta[256]. EN seisukoha preambulis seisab, et nõusoleku andmata jätmise korral võib kasutaja juurdepääsu veebisisule piirata, kui tegemist on nn tasuta teenusega ja kasutajal on võimalik valida sama teenuse osutaja samaväärsete teenuste vahel, millest ühel juhul peab ta küpsistega nõustuma ning teisel juhul mitte. Samas kui see nn samaväärne teenus on tõepoolest samaväärne küpsistega nõustumist eeldava teenusega, siis põhimõtteliselt ei peaks olema tegemist juurdepääsu piiramisega, vähemalt mitte olulises osas. EN seisukoha järgi ei või juurdepääsu piirata, kui tegemist on veebisaitidega, kus pakutakse avaliku sektori teenuseid, või kui esineb poolte selge ebavõrdsus, mh kui teenuse osutajal on domineeriv positsioon, mis ei jäta kasutajale tõelist valikuvabadust[257]. EN seisukoht ei selgita, kuidas plaanitakse domineeriva positsiooni olemasolu tuvastada. Töö autor pooldab põhimõtteliselt nõukogu seisukohta, et teatud juhtudel peaksid küpsisebarjäärid olema keelatud, kuid leiab, et keelu rakendamise tingimused nõuavad täiendavat analüüsi.

Nagu eespool mainitud, on rakenduse kaudu nõusoleku andmist reguleerides oluline tagada, et igale veebisaidile jääks siiski võimalus küsida otse kasutajalt küpsiste salvestamiseks konkreetne nõusolek. Nõusolekut võidakse küsida nii veebisaidi enda kui ka kolmanda osapoole küpsiste salvestamiseks. Kolmanda osapoole küpsiste puhul võib tekkida küsimus, kes peaks nende salvestamiseks kasutajalt nõusoleku küsima. Artikli 29 andmekaitse töörühm rõhutab, et küpsiste kasutamisel peab kasutajalt nõusoleku saama küpsise salvestaja (nõnda ka EN seisukoha pp-is 20aaa), nt reklaamivõrgustik, kes on veebisaitidelt andmete kogumisel, töötlemisel ja muu teabega kombineerimisel vastutav töötleja[258]. Praktikas püütakse olukorras, kus kolmandal isikul ei ole kasutajaga otsekontakti, lahendada nõusoleku küsimise probleem selliselt, et reklaamivõrgustiku ja veebisaidi vahelise lepinguga pannakse viimasele kohustus hankida kasutajalt kehtiv nõusolek, lükates sellega potentsiaalselt osa reklaamivõrgustiku vastutusest veebisaidi õlule. Mõeldes sellele, kui palju on reaalajas toimuvate reklaamipinna oksjonite puhul osapooli, kelle serveritest konkreetse kasutaja andmed (nt profiil) läbi käivad (vt ka ptk 1.3), siis kui iga tarneahela lüli peab saama töötlemiseks kasutajalt nõusoleku, aga seda ei tee, võib olla tegemist mastaapse IKÜM-i rikkumisega.[259]

[256] EP seisukoha art 8 lg 1a.
[257] EN seisukoha pp 20aaaa.
[258] Article 29 Data Protection Working Party. Opinion 2/2010, WP 171, lk 10–11.
[259] Holton, K. Europe's new data law upends global online advertising. – Reuters 23.08.2018. – https://www.reuters.com/article/uk-advertising-gdpr-insight-idINKCN1L80HT (22.04.2021).

Olukorra ebaselgusele on juhtinud tähelepanu Interactive Advertising Bureau (IAB), kes soovitas arvamuses komisjoni 2017. aasta ettepaneku kohta ePM-is selgelt sätestada, et esimene osapool (ehk otsekontakti omaja) võib küsida nõusoleku ka kolmanda osapoole eest[260]. Õiguslikult teise isiku nimel nõusoleku küsimist IKÜM ega EK ja EP seisukohad ette ei näe ning siiani on seda probleemi lahendatud IKÜM-i vastutava-volitatud töötleja ja andmete kolmandale isikule edastamise sätetega[261]. IAB soovitud lahendus aga võib tõeks saada, sest EN seisukoha pp-is 20aaa sätestatakse, et küpsise salvestajaks olev isik (sh reklaamivõrgustik) võib paluda enda nimel kasutajalt nõusoleku küsida muul isikul. Kuigi põhjenduspunktil ei ole artikli siduvust, kasutaksid reklaamitööstuse osapooled seda kindlasti ära. Kolmandale isikule edastamiseks nõusoleku küsimisel tekib siiski küsimus, kas selline nõusolek saab olla teadlik, st kas nõusolekut küsiv veebisait oskab kirjeldada kõiki reklaamivõrgustike poolt tulevikus tehtavaid töötlemistoiminguid ja kas selline nõusolek hõlmab nn neljandale ja viiendale osapoolele edastamist. Nõusoleku teadlikkuse osas soovitatakse veebisaidil ja reklaamivõrgustikul teha omavahel paremat koostööd[262], aga see ei pruugi olla piisav kasutajalt tõeliselt teadliku nõusoleku saamiseks.

Käesoleva alapeatüki kokkuvõtteks on enam-vähem kindel, et uue ePM-i järgi saab olema võimalik hallata nõusolekut rakenduse seadete kaudu, kuid sellega seonduv peamine küsimus – kas vaikimisi hakkavad küpsised olema keelatud või lubatud – selgub läbirääkimiste käigus. Reklaamitööstuse ja selle eri osapoolte jaoks on kahjulikud mistahes meetmed, mis vähendavad nende ligipääsu andmetele, eeskätt range nõusoleku nõue, privaatsust kaitsvad vaikeseaded ja küpsisebarjääride keelustamine. Andmekaitse eestkõnelejad peavad oluliseks nõusoleku rolli isiku eraelu puutumatuse kaitsel ja toetavad vaikimisi privaatsust kaitsvate seadete nõuet. Nad rõhutavad, et kasutajad ei pea leppima küpsiste salvestamise ja jälgimisega ei internetis ega nutiseadmete kaudu, sh väljaspool internetiühendust. Järgmises alapeatükis analüüsitakse uue ePM-i menetluses kaalutavaid erandeid nõusoleku nõudest ehk seda, kas, kes ja millistel juhtudel võib küpsiste abil ja muul viisil kasutaja lõppseadmest andmeid koguda ilma kasutaja nõusolekuta.

[260] Interactive Advertising Bureau Europe (IAB). Position, lk 4.

[261] Muuseas kirjanduses on nõusoleku probleemile lähenetud ka lepinguõiguslikult. Otseturunduse kontekstis on leitud, et kui ettevõte ostab potentsiaalsete uute klientide kontakte sisaldava andmebaasi, siis peaks müüja tagama lepingu eseme kasutatavuse lepingus kokku lepitud eesmärgil. Ehk teisisõnu, kui lepingu esemeks on isikuandmed, peaks müüja olema saanud kõigilt füüsilistelt isikutelt kehtiva nõusoleku nende isikuandmete edastamiseks. Sellega seoses küsimus, kelle omad on isikuandmed ja kuidas on see seotud nt andmebaasi koostaja autoriõigusega. Need küsimused jäävad paraku käesoleva töö raamidest väljaspoole. Leszek, S. Electronic Marketing in the European Union and in the UK – Selected Issues. – International In-House Counsel Journal, Vol. 12, No. 49, Autumn 2019, lk 4.

[262] European Data Protection Board (EDPB). Guidelines 07/2020 on the concepts of controller and processor in the GDPR. Version 1.0. 02.09.2020, lk 43–44.

3.4 Küpsiste ja muude jälgimistehnoloogiate kasutamine ilma kasutaja nõusolekuta

Käesoleva töö kirjutamise ajal kehtiva ePD artikli 5 lg 3 sõnastuse järgi reguleerib säte vaid kasutaja lõppseadmesse teabe „salvestamist" ja sellele „teabele juurdepääsu saamist", mis sobib hästi küpsiste kasutuse reguleerimiseks, kuid ei hõlma selliseid jälgimise viise, mis lõppseadmesse teabe salvestamist ei sisalda. Nt seadme sõrmejälje jäädvustamisel (*device fingerprinting*, vt ka ptk 1.2) kogutakse seadme konfiguratsiooni kohta teavet ja määratakse seadmele identifikaator, kuid seadmesse endasse midagi ei salvestata, mistõttu on see jäänud ePD artikli 5 lg 3 kohaldamisalast välja. Uue ePM-i kohaselt saab tõenäoliselt olema kaitstav igasugune lõppseadmega seotud teave, mis hõlmab mh lõppseadme poolt töödeldavaid andmeid ja seadme tark- ja riistvaraga seotud andmeid[263]. Kehtiva ePD artikli 5 lg 3 kohaselt on ilma nõusolekuta lubatud vaid tehniline teabe salvestamine lõppseadmesse ja juurdepääs sellele, „mille ainus eesmärk on edastada sidet (...) või mis on teenuseosutajale hädavajalik sellise infoühiskonna teenuse osutamiseks, mida abonent või kasutaja on sõnaselgelt taotlenud". Seejuures ei ole kehtiva regulatsiooni järgi hädavajalikud nt analüütikaküpsised, sest kuigi need võivad olla vajalikud veebisaidi haldaja jaoks, ei ole need vajalikud kasutaja soovitud teenuse kasutamiseks, nt soovitud uudise lugemiseks või video vaatamiseks, mis oleksid võimalikud ka ilma analüütikaküpsisteta[264] (vt ka ptk 2.3). Uues ePM-is plaanitakse ühelt poolt lõppseadme kaitset tugevdada, teiselt poolt nähakse ette kehtiva ePD-ga võrreldes rohkem erandeid, mida on mitmed institutsioonid ja huvirühmad küpsisetaotluste vähendamise ja suurema paindlikkuse eesmärgil soovitanud teha[265].

Paljud veebisaidid soovivad teada, kui sageli nende saiti külastatakse, milliste otsisõnade kaudu nende veebisaidile satutakse, milliseid saidi alamlehti kasutajad kõige sagedamini ja kauem külastavad jms. Veebisait ise saab kasutajate tegevust analüüsida esimese osapoole küpsiste abil, olles ise küpsise salvestajaks ja selle kaudu teabe kogujaks. Et paljudel veebisaitidel endil ei ole otstarbekas veebianalüütika tegemiseks meeskonda palgal hoida, tellitakse seda teenust sageli kolmandalt isikult. Üks võimalus on edastada kolmandast isikust teenusepakkujale analüüsimiseks veebisaidi enda ehk esimese osapoole küpsistega kogutud teave. Teine variant on kasutada kolmanda osapoole küpsiseid ja analüüsiteenuseid, st veebisaidi külastaja arvutisse salvestab küpsise kolmas isik, kes ka kogub ja analüüsib saadud andmeid.[266] Kolmandaks isikuks on sageli reklaamitööstuse eri osapooled, kes soovivad oma

[263] EK, EP ja EN seisukohtade art 2 ja art 8.
[264] Article 29 Data Protection Working Party. Opinion 04/2012, WP 194, lk 10.
[265] European Data Protection Supervisor. Opinion 5/2016, lk 17; Article 29 Data Protection Working Party. Opinion 01/2017, WP 247, lk 18; Mozilla position paper, lk 4.
[266] Article 29 Data Protection Working Party. Opinion 04/2012, WP 194, lk 10.

partnerveebisaitide kaudu kasutajate kohta teavet koguda, et mõõta reklaamide esitamise ja reklaamikanalite edukust[267]. Kolmanda isiku kasutamisel on oht eraelu puutumatusele reeglina suurem[268].

Nii EK, EP kui ka EN seisukohas nähakse ette võimalus koguda ilma kasutaja nõusolekuta lõppseadmega seotud andmeid teatud tingimustel teenuse külastajate arvu mõõtmiseks (*audience measuring*). EK seisukohas[269] on teabe kogumine veebis külastajate arvu mõõtmiseks (ehk nn statistika erand) ilma kasutaja nõusolekuta lubatud vaid kasutaja soovitud infoühiskonna teenuse osutaja enda poolt, kuid edastamine kolmandale isikule ilma kasutaja nõusolekuta on keelatud. EK sedavõrd jäik positsioon ei haaku hästi veebisaitide praktiliste vajadustega, sest veebisaidi omanikud tellivad külastajate arvu ja veebisaidi ülesehituse optimeerimise analüüsi sageli mõnelt veebianalüütikat pakkuvalt ettevõtjalt[270]. EK seisukoht tähendaks seda, et kui veebisait ise veebianalüütikat läbi ei vii, siis ta statistika erandile tugineda ei saaks ja tal oleks võimalik oma saidi efektiivsust mõõta ja optimeerida vaid kasutaja nõusolekul.

EP seisukoha[271] järgi võib teenuse külastajate arvu mõõtmiseks lõppseadmest andmeid koguda kahel tingimusel. Esiteks tingimusel, et mõõtmist teostab: (a) teenuse osutaja ise; (b) kolmas isik teenuse osutaja nimel; või (d) veebianalüüsi agentuur, kes tegutseb avalikes huvides, sh teaduslikul eesmärgil. Teiseks tingimusel, et: (1) andmed on koondatud (*aggregated*); (2) kasutajale on antud võimalus esitada vastuväide; (3) isikuandmeid ei tehta kättesaadavaks ühelegi kolmandale isikule; ja (4) kõnealune mõõtmine ei kahjusta kasutaja põhiõigusi. Juhul kui külastajate arvu mõõtmine toimub infoühiskonna teenuse osutaja nimel (ülal variant b) kehtib veel kaks täiendavat tingimust: (i) andmeid võib töödelda ainult selle teenuse osutaja jaoks ning (ii) andmeid peab hoidma eraldi andmetest, mis on kogutud külastajate arvu mõõtmiseks teiste teenuse osutajate jaoks. EP seisukoht pakub veebisaitidele rohkem võimalusi saidi toimimise kohta tagasiside saamiseks, võttes samas meetmeid kasutajate kaitseks, kuigi võiks küsida, miks ei ole nende meetmete hulgas andmete anonüümimise kohustust. Veebisaidi kasutuse analüüsimiseks ei pea üksikisik olema tuvastatav, vaid olulisem ongi see, kui palju kasutajaid saidil teatud artiklit luges, mitte kes täpselt seda artiklit luges.

EN seisukoha järgi võib lõppseadmega seotud andmeid koguda teenuse külastajate arvu mõõtmiseks tingimusel, et mõõtmist teeb: (a) kasutaja soovitud teenuse osutaja; (b) kolmas isik

[267] Competition and Markets Authority. Online platforms and digital advertising Market study final report. London, 2020, lk 267.
[268] Article 29 Data Protection Working Party. Opinion 04/2012, WP 194, lk 10.
[269] EK seisukoha art 8 lg 1 p d.
[270] European Data Protection Board (EDPB). Guidelines 07/2020, lk 25.
[271] EP seisukoha art 8 lg 1 p d.

teenuse osutaja nimel; (c) kolmandad isikud ühiselt teenuse osutaja nimel; või (d) kolmas isik ja kasutaja soovitud teenuse osutaja ühiselt. Kolmandate isikute kaasamisel peavad olema täidetud IKÜM-i artikli 26 või 28 nõuded, mis näevad ette reeglid kaasvastutavate töötlejate ja volitatud töötleja jaoks. On küll positiivne, et EN seisukoht viitab IKÜM-i regulatsioonile, kuid reaalsuses võib vastutava ja volitatud töötleja määramine olla keeruline.

Volitatud töötleja tohib töödelda vastutavalt töötlejalt ehk nt veebisaidilt saadud andmeid üksnes veebisaidi määratud eesmärkide ja juhiste järgi ning mitte ühelgi muul eesmärgil (IKÜM art 28). Kui veebisait sõlmib veebianalüütikateenuse pakkujaga lepingu, milles sätestatakse, et veebianalüütikateenuse pakkuja kogub ja analüüsib andmeid külastajate tegevuse kohta veebisaidil ning et ta on selles õigussuhtes volitatud töötlejaks, siis juhul kui veebianalüütikateenuse pakkuja kasutab veebisaidi külastajate andmeid ühtlasi muudel eesmärkidel, nt oma äritegevuse ja muude teenuste edendamiseks, loetakse veebianalüütikateenuse pakkuja selle tegevuse suhtes vastutavaks töötlejaks (IKÜM art 28 lg 10), sest selle tegevuse raames määrab ta ise töötlemise eesmärgid ja vahendid[272]. St et lisaeesmärkidel töötlemiseks peab veebianalüütikateenuse pakkuja saama kõigilt veebisaidi külastajatelt nõusoleku ja täitma kõiki vastutavale töötlejale õigusaktidest tulenevaid nõudeid. Seda juhul, kui veebisaidi külastajate andmed on isikuandmed, kuid võttes näiteks kõige levinuma[273] veebianalüütikateenuse pakkuja Google Analytics'i, siis nende veebisaidil on esitatud teave, et Analytics on loodud töötama koos Google'i reklaamiteenustega (nii reklaamija kui ka veebisaidi poolel), selleks et teenuse tellija saaks kasutada veebianalüütikast pärit teavet õigete klientideni jõudmiseks[274]. Õigete klientideni jõudmine ilmselt eeldab nende isikuandmete kogumist ja töötlemist.

EN seisukoht sätestab veel ühe erandi, mida EK ja EP seisukohtades ei ole. Nimelt lubab EN seisukoht[275] küpsistega kogutud andmeid muul eesmärgil ilma kasutaja nõusolekuta edasi töödelda (*further processing*), kui muu eesmärk on kooskõlas (*compatible*) esialgse eesmärgiga, lähtudes sisuliselt IKÜM-i artikli 6 lg 4 põhimõtetest. Seda tingimusel, et (i) küpsistega kogutud andmed hiljem kustutatakse või anonüümitakse; (ii) töödeldakse vaid pseudonüümitud andmeid; ja (iii) lõppseadme andmeid ei kasutata kasutaja olemuse või tunnuste kindlaksmääramiseks ega tema profileerimiseks. Lisaks EN seisukoha art 8 lõigete g ja h keerulisele sõnastusele, on lõikes h (ehk eelmises lauses) esitatud tingimused vastuolulised, sest kui kõigepealt tuleb andmed kustutada või anonüümida (i), siis ei saa sellele enam järgneda

[272] European Data Protection Board (EDPB). Guidelines 07/2020, lk 19, 25.
[273] Hotjar. Top 20 web analytics tools from our survey of 2000+ experts. (06.04.2021) – https://www.hotjar.com/web-analytics/tools/ (24.04.2021); Horne, K. 22 Top Website Analytics Tools To Grow Sales. (22.10.2020). – https://digital.com/web-analytics-software/ (24.04.2021).
[274] Google Marketing Platform. Analytics. – https://marketingplatform.google.com/about/analytics/ (17.02.2021).
[275] EN seisukoha art 8 lg 1 p-d g ja h.

andmete pseudonüümimine (ii). Lisaks võimaldab EN seisukoht edastada andmeid edasiseks töötlemiseks kolmandale isikule juhul, kui kolmas isik on IKÜM-i järgi volitatud töötleja või andmed on anonüümitud (art 8 lg 1 p i).

Ühelt poolt annab EN seisukohas edasise töötlemise lubamine ilma kasutaja nõusolekuta EK ja EP seisukohtadega võrreldes kasutajale nõrgema kaitse, sest sellel erandil on mitu hinnangulist etappi. Nt eesmärkide vahelise kooskõla väljaselgitamine on tõlgendamise küsimus, mis võib õõnestada ePM-iga antavat kaitset, sest lõppastmes otsustab kooskõla üle andmetöötleja ise. Samale probleemile juhtis tähelepanu ka Euroopa Andmekaitsenõukogu, kes toetab EK ja EP seisukohtade üldisi keelde koos kitsaste eranditega[276]. Teiselt poolt, arvestades EN seisukohas on sätestatud kaitsemeetmeid, eriti andmete anonüümimise kohustust, isiku profileerimise ja tema olemuslike tunnuste tuvastamise keeldu, ei peaks sel erandil olema kasutaja isikuandmete töötlemisele suurt mõju. Siiski tekib küsimus, kas esialgse eesmärgiga kooskõlas oleval muul eesmärgil töötlemiseks on erandit vaja, arvestades, et küpsistega kogutud isikuandmeid võib ilma nõusolekuta töödelda niipea, kui need on pöördumatult anonüümitud[277].

EK, EP ja EN seisukohtadest jääb mulje, et anonüümimist peetakse heaks alternatiiviks olukorras, kus nõusolekule ei ole võimalik tugineda, kuid andmeid oleks vaja töödelda. IKÜM-i järgi tähendab anonüümimine anonüümseks muutmist „sellisel viisil, et andmesubjekti ei ole võimalik tuvastada või ei ole enam võimalik tuvastada" (pp 26). Õiguskirjanduses täiendatakse sõna „anonüümne" sageli sõnadega „tõeliselt" või „täielikult" , mis tekitab küsimuse, kas andmed saavad olla osaliselt anonüümsed. Artikli 29 andmekaitse töörühm on juhtinud tähelepanu asjaolule, et anonüümimine ei ole ühekordne tegevus[278], eriti tehisintellekti ja algoritmiliste korrelatsioonide kasutamise kontekstis[279]. Anonüümimiseks saab ja tuleb kasutada eri tehnikaid koos ning arvestada võimalusega, et andmed, mis on nende koguja poolt anonüümitud, võivad kolmandale isikule edastamisel muutuda taas isiku tuvastamist võimaldavateks andmeteks.

Mis puutub muude jälgimistehnoloogiate kasutamisse ilma kasutaja nõusolekuta, siis nende puhul on plaanitavad erandid avaramad kui küpsiste kasutamise puhul. EK, EP ja EN seisukohad lubavad ilma kasutaja nõusolekuta töödelda lõppseadme poolt välja saadetavat teavet (nt ultraheli- või raadiosignaali) tingimusel, et (1) kasutajale esitatakse hästi nähtav teave sellise andmekogumise kohta kohas, kus masinatevaheline suhtlus toimub; (2) andmeid

[276] European Data Protection Board (EDPB). Statement 03/2021, lk 4.
[277] European Data Protection Board (EDPB). Statement 03/2021, lk 4.
[278] Article 29 Data Protection Working Party. Opinion 05/2014 on Anonymisation Techniques. 0829/14/EN, WP 216, 10.04.2014, lk 3–4.
[279] OECD. Artificial Intelligence in Society, lk 87.

kogutakse üksnes statistilisel eesmärgil ja kustutatakse või anonüümitakse pärast eesmärgi täitmist (ainult EP ja EN seisukohad); ning (3) kasutajal on õigus esitada vastuväide, kui see ei mõjuta lõppseadme funktsionaalsust (ainult EP seisukoht), või kasutajat teavitatakse meetmetest, mida ta saab võtta, et peatada või vähendada andmekogumist (EK ja EN seisukohad)[280].

Need sätted puudutavad esmajoones masinatevahelise side najal toimivat asjade internetti (IoT), mille puhul nt veebisaiti sisse kodeeritud ultrahelisignaal edastab läheduses olevale mikrofoniga seadmele teate, et kasutaja viibib parasjagu vastaval veebisaidil, või nt arukas külmkapp saadab reklaamivahendajale teavet kasutaja toitumisharjumuste kohta või tellib kauplusest omal algatusel piima, kui see külmkapist otsa saab[281] (vt ka ptk 1.2). EK ja EN seisukohas mainitud võimalust üksnes vähendada, aga mitte vältida andmekogumist on nimetatud ka nõrgaks loobumise võimaluseks (*weak opt out*)[282], sest tegelikult ei jää sellisel juhul kasutajal muud üle kui loobuda selliste seadmete kasutamisest või sellises kohas, nt ultrahelisignaali kasutavas kaupluses viibimisest. Masinatevahelise side puhuks ettenähtud erandid on ilmselt mõeldud asjade interneti teenuste edasiarendamiseks, kuid ka sel juhul on tarvis lahendada küsimus isikuandmete muul eesmärgil edasise töötlemise lubatavusest[283]. Käesoleva töö autor leiab, et kasutajal peaks alati olema võimalus isegi statistilisel eesmärgil andmekogumisest keelduda.

Kokkuvõttes lubavad EK, EP ja EN seisukohad ilma kasutaja nõusolekuta koguda küpsiste abil andmeid veebianalüütika eesmärgil (jättes kõrval muud, reklaamitööstuse kontekstis väheolulised erandid). Statistika erandil on positiivne mõju veebisaitidele, kes tõenäoliselt saavad uue ePM-i alusel ilma kasutaja nõusolekuta koguda andmeid veebisaidi või rakenduse (anonüümse) kasutusstatistika tegemiseks ning seeläbi oma teenuste parendamiseks ja optimeerimiseks. Veebianalüütika erandiga on seotud küsimus, kes seda analüüsi läbi viib. EK seisukoht lubab veebianalüütika erandi alusel küpsiste abil andmeid koguda ainult veebisaidil endal. EP seisukoht lubab küpsistega kogutud andmeid kolmandale isikule edastada vaid kitsastes raamides, sh kohustades veebianalüütikateenuse pakkujat hoidma ühelt veebisaidilt saadud andmed eraldi teistelt veebisaitidelt saadud andmetest. EN seisukoht viitab andmete kolmandale isikule edastamisel küll IKÜM-i vastutava-volitatud töötleja regulatsioonile, kuid praktikas esineb oht, et veebianalüütikateenuse pakkuja kasutab veebisaidilt saadud andmeid ka laiemalt reklaamitööstuse huvides isikute jälgimiseks.

[280] EK seisukoha art 8 lg 2 p b; EP seisukoha art 8 lg 2a–2b; EN seisukoha art 8 lg 2–2a.
[281] Zuiderveen Borgesius. Personal data processing for behavioural targeting, lk 167.
[282] Specht, Kerber, lk 149.
[283] Article 29 Data Protection Working Party. Opinion 8/2014, WP 223, lk 7–8.

3.5 Menetletava e-privaatsuse määruse jõustamine

Käesoleva töö kirjutamise ajal kehtiva ePD sätete kohta on öeldud, et kui olemasolevaidki reegleid täidetaks, oleks andmekaitse tase EL-is parem[284]. Sears kirjutas 2019. aastal, et kuigi mitmed veebilehitsejad võimaldavad keelduda kolmanda osapoole küpsistest, on paraku palju veebisaite, kes neid seadeid ja seega kasutajate soove ei austa, samuti tehnoloogiaid, mis suudavad kustutatud küpsised taasluua[285].

Ühest 2012. aastal läbi viidud uuringust selgus, et vaatamata Google'i kinnitustele, et ta austab kasutajate küpsiste seadeid, ja Google'i enda loodud küpsiste blokeerija reklaamimisele, oli Google jätkuvalt salaja programmeerinud veebilehitsejaid kolmanda osapoole küpsiseid lubama[286]. 2021. aasta märtsis teatas Google, et plaanib loobuda kasutajate veebitegevuse jälgimisest üksikisiku tasandil ning hakata selle asemel reklaame kuvama sarnase sirvimisajalooga kasutajate gruppi kuuluvatele isikutele. Küpsiste asemel kasutatav uus mehhanism nimega FloC jälgiks seega teatud kasutajate rühma, mitte üksikisikuid. Samas leiavad andmekaitse eestkõnelejad, et sellel tehnoloogial võib olla hoopis vastupidine mõju: kui andmeid koguv reklaamitööstuse osapool saab teada rühma(d), kuhu kasutaja kuulub, on pool tema tööst juba tehtud[287]. On raske uskuda, et tegemist pole lihtsalt järjekordse, olgugi modifitseeritud jälgimistehnoloogiaga.

Kui üle kahekümne aasta jälgimistehnoloogiate tipus võidutsenud kolmanda osapoole küpsis tõepoolest peagi uuema tehnoloogia vastu välja vahetatakse, on seda olulisem käesoleva töö kirjutamise ajal menetletava uue ePM-iga tagada, et määrus ei oleks selle vastuvõtmise ajaks juba vananenud, nagu juhtus esimese, 1997. aastal vastu võetud side konfidentsiaalsuse direktiiviga, mida menetleti seitse aastat. Mozilla hoiatab oma seisukohas komisjoni 2017. aasta ettepanekule liigselt konkreetsetele tehnoloogiatele, nagu kolmanda osapoole küpsised, keskendumise eest, ning soovitad reguleerida rohkem printsiibipõhiselt. Tähelepanu peaks pöörama ohule, mida soovitakse ära hoida, sest eesmärk on keelustada ilma isiku nõusolekuta ja hädavajaduseta tema jälgimine, sõltumata jälgimise viisist.[288] Käesoleva töö autor nõustub

[284] Article 29 Data Protection Working Party. The Future of Privacy, lk 2; Hogan & Hartson LLP, lk 291.
[285] Sears, A. M. The Limits of Online Price Discrimination in Europe. – Columbia Science and Technology Law Review, Vol. 21, No. 1, Fall 2019, lk 23; Article 29 Data Protection Working Party. Opinion 2/2010 on online behavioural advertising, lk 14.
[286] Jones, Lee, lk 112.
[287] Cyphers, B. Google's FLoC Is a Terrible Idea. – Electronic Frontier Foundation (03.03.2012) – https://www.eff.org/deeplinks/2021/03/googles-floc-terrible-idea (24.04.2021); Randlo, T. Google katsetab uut kasutajate jälgimise viisi: kontrolli, kas oled testrühmas. – Postimees 14.04.2021. – https://majandus24.postimees.ee/7225007/google-katsetab-uut-kasutajate-jalgimise-viisi-kontrolli-kas-oled-testruhmas?_ga=2.73232659.1814441037.1618472410-1340925722.1567145559 (15.04.2021).
[288] Mozilla position paper, lk 7, 9.

sellega, et uue ePM-i sõnastus peaks olema piisavalt avar, ent leiab, et printsiipidele lisaks oleks vaja luua õiguslik alus vajadusel neid printsiipe kohustatud isikutele siduvalt täpsustada.

Jonesi ja Lee[289] viidatud Ron Wydeni USA Senatile esitatud seaduseelnõus (vt ka ptk 3.3) pakuti välja, et kasutajad võiksid saada kõiki jälgimisega seotud seadeid hallata ühel veebisaidil, mida haldaks Federal Trade Commission. Käesoleva töö autor leiab, et sarnaselt peaks uues ePM-is selgelt määrama teatud sätete, nt privaatsust suurendavate tehniliste standardite väljatöötamise ja rakendamise eest vastutava isiku või asutuse. Seda küsimust on käsitletud üksnes EP seisukohas, milles tehakse Euroopa Andmekaitsenõukogule ülesandeks mh anda välja suuniseid selle kohta, kuidas edastab rakendus (nt veebilehitseja) teistele osapooltele signaali kasutaja tehtud privaatsussätete kohta, ning anda välja suuniseid, soovitusi ja parimaid tavasid infoühiskonna teenuse kasutajate arvu mõõtmise, lõppseadme poolt edastatava teabe töötlemise ja rakenduse kaudu antava nõusoleku kohta[290]. EK ja EN seisukohtades niivõrd konkreetseid sätteid kahjuks ei ole.

Vajadust kehtestada tark- ja riistvaratootjatele eraelu puutumatust kaitsvad siduvad nõuded on korduvalt rõhutatud alates 1990. aastate lõpust[291], 2009. aasta paiku[292] ning nüüd uue ePM-i menetlemisel[293]. Artikli 29 andmekaitse töörühm tegi 2009. aastal komisjonile soovituse sätestada üldine lõimitud andmekaitse põhimõte (käesoleva töö kirjutamise ajal IKÜM art 25), kuid täpsustas samas, et info- ja kommunikatsioonitehnoloogia valdkonnas on lisaks üldisele lõimitud andmekaitse põhimõttele vaja praktilisemat ja konkreetsemat lähenemist teatud kasutusjuhtudele suunatud eeskirjade näol[294]. Ka see mõte ei ole uudne: 2002. aasta direktiivi artikli 14 lg-s 3 on ette nähtud võimalus võtta vajaduse korral vastu „meetmeid tagamaks, et lõppseadmete konstrueerimine on kooskõlas kasutajate õigusega kaitsta oma isikuandmeid ja kontrollida nende kasutamist". See säte viitab lõppseadmena üksnes raadioseadmetele, kuid uue ePM-i kontekstis laieneks see kõigile elektroonilist sidet (nt internetiühendust) võimaldavatele lõppseadmetele.

Kokkuvõttes võib öelda, et enamik EK, EP ja EN seisukohtades välja pakutud lahendusi ei ole põhimõtteliselt uued ideed, vaid käesoleva töö autori arvates pigem varem tegemata

[289] Jones, Lee, lk 129.
[290] EP seisukoha art 19 lg 1 p-d bb ja bd.
[291] Article 29 Data Protection Working Party. Recommendation 1/99, lk 1–5; Article 29 Data Protection Working Party. Opinion 7/2000 on the European Commission Proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector of 12 July 2000 COM (2000) 385. 5042/00/EN/FINAL, WP 36, 02.11.2000, lk 10.
[292] Article 29 Data Protection Working Party. The Future of Privacy, lk 12–15.
[293] Article 29 Data Protection Working Party. Opinion 03/2016 on the evaluation and review of the ePrivacy Directive, lk 18–19; Article 29 Data Protection Working Party. Opinion 01/2017 on the Proposed Regulation for the ePrivacy, lk 14; European Data Protection Board (EDPB). Statement of the EDPB on the revision of the ePrivacy Regulation, lk 3.
[294] Article 29 Data Protection Working Party. The Future of Privacy, lk 12, 15.

jäänud töö. Käesoleva töö analüüs näitab, et üleskutseid on tehtud korduvalt, kuid need ei ole andnud tulemust. Ilmselt on tulutu julgustada tarkvaratootjaid tegema endale äriliselt mitte just kasulikke otsuseid, kuid uue määrusega olulise mõju saavutamiseks on tarvis alustada ahela algusest. Käesoleva töö autor on veendunud, et kui tarkvara jälgimiskindlaks muutmine jääb ePM-i preambulis tungiva soovituse tasandile ilma siduva artiklita ja sätete üle järelevalve tegija määramiseta (nagu siiani ePD-s, vt ptk 2.2), ei ole suurt põhjust muutusi oodata. On arusaadav, et kirjutada ette andmekaitsenõudeid globaalse haardega suurkorporatsioonidele, nagu Microsoft, Google ja Apple, võib tunduda hulljulge või isegi hukule määratud ettevõtmisena, aga küsimus on, mis on eesmärk ja kus soovib Euroopa olla kümne ja kahekümne aasta pärast. Tehniliste standardite ja ohutuspõhimõtete järgimine on toote- ja teenusedisaini lahutamatu osa, mis ei põhine üksnes hea tahte protokollidel.

Otsustavat jõustamist vajavad muidugi ka muud sätted. Kuigi EK, EP ja EN seisukohad[295] näevad ette teatavad volitused liikmesriikide järelevalveasutustele, mis arvatavasti saavad olema samad asutused, kes teevad järelevalvet IKÜM-i üle, siis käesoleva töö autori arvates tasub kaaluda suurema mõjujõuga üleeuroopaliselt tegutsevate teenuse osutajate üle järelevalve tegemise koordineerimist liidu tasandil, volitades selleks nt Euroopa Andmekaitseinspektorit, kelle ülesanded praegu hõlmavad vaid järelevalvet isikuandmete töötlemise üle EL-i institutsioonide ja organite poolt[296] või luua selleks muu selge ja praktiline mehhanism. Nagu IKÜM nägi ette kohustuse viia üldmääruse kohaldamise alguskuupäeval käimasolev töötlemine üldmäärusega kooskõlla kahe aasta jooksul üldmääruse jõustumisest alates (pp 171), nõnda peaks uus ePM sätestama sarnase kohustuse, arvestades käesolevas töös korduvalt esile toodud küpsiste ja muude jälgimistehnoloogiate abil kogutud andmete massilist töötlemist.

Reklaamitööstus on küpsiste loomisest ehk 1990. aastate teisest poolest saadik tugevalt survestanud regulaatoreid mitte kehtestama neile kahjulikke nõudeid, rõhudes eneseregulatsiooni ja nn pehmete meetmete (*soft law*) suuremale paindlikkusele[297]. Paraku on direktiivide mõjuhinnangutes aja jooksul korduvalt järeldatud, et eneseregulatsioon ei toimi[298],

[295] Kõigi seisukohtade art 18.
[296] 23. oktoobri 2018 Euroopa Parlamendi ja nõukogu määrus (EL) 2018/1725, mis käsitleb füüsiliste isikute kaitset isikuandmete töötlemisel liidu institutsioonides, organites ja asutustes ning isikuandmete vaba liikumist, ning millega tunnistatakse kehtetuks määrus (EÜ) nr 45/2001 ja otsus nr 1247/2002/EÜ. – ELT L 295, 21.11.2018, lk 39–98, art 52jj.
[297] Kristol, lk 163; Amnesty International, lk 48.
[298] Seda nenditi nii 2009. aasta direktiivi kui ka käesoleva ePM-i reformi käigus. European Commission. Impact Assessment Accompanying document to the Proposal for a Directive of the European Parliament and the Council amending European Parliament and Council Directives 2002/19/EC, 2002/20/EC and 202/21/EC; Proposal for a Directive of the European Parliament and the Council amending European Parliament and Council Directives 2002/22/EC and 2002/58/EC; Proposal for a Regulation of the European Parliament and the Council establishing the European Electronic Communications Markets Authority. SEC(2007) 1472. Brussels, 13.11.2007, lk 108;

mida olekski ausalt öeldes naiivne loota, arvestades, et andmetega kauplemise mistahes piiramine on reklaamitööstusele kahjulik. Reklaamitööstusele vastutulemine ja kasumile orienteeritud osapoolte heale tahtele lootmine[299] on üheks põhjuseks, miks isikute eraelu puutumatuse riive on käesoleval hetkel sedavõrd intensiivne, kuigi see võib üksikisiku tasandil ja üksiku töötlemistoimingu kontekstis olla raskesti hoomatav[300].

Zuiderveen Borgesius jt ning Kristol on juhtinud tähelepanu sellele, et käitumispõhine reklaam ei ole ainus reklaamimise viis. Kolmanda osapoole küpsiste vaikimisi keelamine ähvardab reklaamitööstuses levinud *ärimudeleid*, mis rajanevad isikute jälgimisel, kuid mitte reklaamide esitamist veebis põhimõtteliselt[301]. Õiguskeskkonna muutus on tavapärane äririsk, millega peab arvestama igas majandusharus. Ettevõtjad, kes investeerivad aega ja raha isikuandmete aina uute ja tulutoovamate kasutamisviiside leiutamisse, võiksid samasuguse innu ja innovaatilise mõtteviisiga läheneda andmekaitse põhimõtete rakendamisele[302].

Kui võrrelda käesoleva töö keskmes olnud küpsiste ja muude jälgimistehnoloogiate kasutuse regulatsiooni ühe teise, samuti ePM-i kohaldamisalasse kuuluva äripraktikaga, nimelt otseturundusega, siis soovimatud reklaamkõned (*unsolicited communications*) on olnud ilma kasutaja nõusolekuta keelatud alates 1997. aasta direktiivist, sest nii lihtsalt otsustati. 2002. aasta direktiivis leiti, et soovimatute turundusteadete saatmine võib küll olla lihtne ja odav, kuid see võib põhjustada saajale kulutusi ning koormata üle nii saaja kui ka elektroonilise side võrgud (pp 40). Seadusandjad leidsid, et automatiseeritud otseturunduskõned on häirivad ja toovad enam kahju kui kasu[303]. Isikute jälgimine kommertseesmärkidel on samamoodi soovimatu, häiriv ja eraellu tungiv. Tahaks loota, et nõnda nagu 2009. aastal kehtestati eelneva nõusoleku nõue – ehk sisuliselt vaikimisi küpsiste keelamise kohustus – veebisaidi tasandil, nõnda sätestatakse uues ePM-is vaikimisi küpsiste keelamine veebilehitseja tasandil.

Lõppastmes ei ole küpsiste ja muude jälgimistehnoloogiate reguleerimine mitte õiguslik ega tehniline küsimus, mida mõistis Kristol juba 1990. aastate lõpus küpsiste standardeid välja töötades, vaid poliitiline väärtusküsimus[304]. Harvardi ülikooli professor Zuboff kirjutab, et

---

European Commission. Impact Assessment. SWD(2017) 3 final. Part 1/3, lk 27; Article 29 Data Protection Working Party. Opinion 2/2010 on online behavioural advertising, lk 22; Euroopa Komisjon. Ettepanek: COM(2017) 10 final, 2017/0003 (COD), ptk 2.3.

[299] Meenutades peatükis 1.2 kirjeldatud Facebooki patenteeritud jälgimistehnoloogiaid kasutajatele sõbrasoovituste tegemiseks, on Facebooki heale tahtele lootmine sellises olukorras naiivne. Mattu, Hill.

[300] European Data Protection Supervisor. Second opinion of the European Data Protection Supervisor on the review of Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). – OJ C 128, 06.06.2009, lk 39.

[301] Kristol, lk 160–161, 163.

[302] European Data Protection Supervisor. Opinion 7/2015. Meeting the challenges of big data. A call for transparency, user control, data protection by design and accountability. 19.11.2015, lk 14.

[303] Tene, Polonetsky, lk 287.

[304] Tene, Polonetsky, lk 286–187, Kristol, lk 167.

ühiskonnad on ajaloo jooksul kuulutanud õigusvastaseks mitmesuguseid moraalselt vastuvõetamatuid tegevusi, nagu inimorganite, laste ja orjadega kaubitsemine[305]. Euroopa Andmekaitseinspektor on öelnud, et pelk asjaolu, et isikuandmetega kauplemise turg on olemas, ei tähenda, et selle peaks heaks kiitma seaduse tasandil. Samamoodi ei õigusta inimorganitega kaubitsemist tõsiasi, et seda tehakse[306]. Käesoleva töö autor nõustub sellega, et inimeste eraelulisi asjaolusid ekspluateerivatel ärimudelitel ei peagi ühiskonnas kohta olema. Nõnda nagu sadakond aastat tagasi ühinesid vabrikutöölised võitlema endale välja paremaid töötingimusi, nõnda tuleb üksikisikutel käesoleval ajal võidelda endale välja ühiskond, mida ei dikteeri jälgimiskapitalism[307]. Käesoleva töö autor loodab, et eraelu puutumatuse kaitse ei ole Euroopas kümne-kahekümne aasta pärast samas või veel viletsamas seisus, vaid et suudame leida nõu ja jõu oma põhiväärtuste eest seista.

Käesolevas alapeatükis analüüsiti peamisi vaidlusküsimusi küpsiste ja muude jälgimistehnoloogiate reguleerimisel käesoleva töö kirjutamise ajal menetletavas ePM-is. Üks olulisemaid muudatusi kehtiva ePD-ga võrreldes saab olema nõusoleku andmise võimalus rakenduse (nt veebisaidi) seadetes, mille eesmärk on vähendada nõusolekutaotluste arvu ning muuta kasutajakogemus veebikeskkonnas, aga ka mobiili- ja muudes rakendustes, sujuvamaks. Eri seisukohtadel on EK, EP ja EN selles, millised peaksid olema rakenduste vaikeseaded. Arvestades vaikeseadete mõju inimkäitumisele, on käesoleva töö autor seisukohal, et vaikimisi ja lõimitud andmekaitse on hädavajalikud tõelise muutuse esilekutsumiseks. EP seisukoht konkretiseerib IKÜM-i lõimitud andmekaitse põhimõtet, nähes ette tark-ja riistvaratootjate kohustuse pakkuda privaatsust soodustavaid tooteid ja teenuseid. Vaieldav on see, kas teenuse osutaja võib keelata teenusele juurdepääsu kasutajale, kes ei nõustu küpsiste või muude jälgimistehnoloogiate kasutamisega või alternatiivselt teenuse eest tasumisega. Et kehtiva ePD üks puudusi on selle ebaühtlane jõustamine, toetab käesoleva töö autor konkreetsete normide jõustamiseks vastutavate isikute määramist ja nende volitamist vajadusel ePM-i täpsustavate siduvate otsuste vastuvõtmiseks (nt tehniliste standardite väljatöötamiseks). Kõigile eespool nimetatud ettepanekutele võitleb tuliselt vastu reklaamitööstus, kes näeb vaikimisi privaatsust kaitsvates rakenduse seadetes ja küpsisebarjääride keelustamises õigustatult ohtu isikute laiaulatuslikul jälgimisel põhinevatele ärimudelitele. Käesoleva töö autor leiab siiski, et ühe isiku ärihuvid ei saa kaaluda üles teise isiku põhiõigusi. Oma tooteid ja teenuseid on võimalik turundada ka ilma isikute eraelu jälgimiseta.

[305] Zuboff, S. You Are Now Remotely Controlled. Surveillance capitalists control the science and the scientists, the secrets and the truth. – The New York Times 24.01.2020. – https://www.nytimes.com/2020/01/24/opinion/sunday/surveillance-capitalism.html (14.02.2021).
[306] European Data Protection Supervisor. Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content. 14.03.2017, lk 7.
[307] Zuboff 2020.

Kokkuvõte

Käesolevas töös otsiti lahendust probleemile, kuidas tõsta töö kirjutamise ajal menetletavas e-privaatsuse määruses küpsiste ja muude jälgimistehnoloogiate reguleerimisel eraelu puutumatuse kaitse taset EL-is, arvestades seejuures võimalust mööda reklaamitööstuse huvidega. Magistritöö eesmärk oli pakkuda küpsiste ja muude jälgimistehnoloogiate reguleerimiseks välja lahendusi, mis tooksid kaasa muutuse, oleksid praktikas rakendatavad ning mille abil isikute eraelu puutumatus oleks kaitstud ja samas andmetöötlus, mis isikute õigusi ei riiva, saaks toimuda. Töös püstitati järgmised uurimisküsimused:

(1) Mis on küpsised ja muud jälgimistehnoloogiad ja millised on neist lähtuvad ohud eraelu puutumatusele seoses nende kasutusega reklaamitööstuses?
(2) Kuidas on küpsiste ja muude jälgimistehnoloogiate kasutamist EL-is siiani reguleeritud ning millistel tingimustel tohib kehtiva regulatsiooni kohaselt küpsiste ja muude jälgimistehnoloogiate abil koguda andmeid veebi ja nutiseadmete kasutajate kohta?
(3) Millised on peamised vaidlusküsimused menetletavas e-privaatsuse määruses küpsiste ja muude jälgimistehnoloogiate reguleerimisel ja millised oleksid neile sobivad lahendused?

Vastusena esimesele uurimisküsimusele leiti, et küpsis on tähtedest ja numbritest koosnev tekstifail, mille veebilehitseja salvestab kasutaja arvutisse, et pidada meeles kasutajaga seotud teavet, nagu teenusesse sisselogimise andmed (e-posti või internetipanga kasutajatunnus ja parool) või e-poes ostukorvi asetatud tooted. Need on kaks näidet vajalikest küpsistest, ilma milleta veebisait ei toimiks. Nt kasutaja peaks iga kord uuesti sisse logima, kui ta vajutab internetipangas „Tagasi" nuppu. Peale vajalike küpsiste eristatakse tavaliselt veel kolme liiki küpsiseid: analüütika-, eelistuste ja turundusküpsised. Lisaks võivad küpsised olla parasjagu külastatava veebisaidi ehk esimese osapoole küpsised või kolmanda osapoole nt reklaamivõrgustiku küpsised. Reklaamivõrgustikud salvestavad küpsiseid sageli selliselt, et kui kasutaja külastab reklaame sisaldavat veebilehte (nt uudisteportaali), siis iga üksiku reklaami kuvamiseks saadab veebilehitseja päringu vastavat reklaami hoiustavale serverile, kes saadab vastu küpsise, mis salvestatakse kasutaja arvutisse, või täiendab kasutaja kohta juba olemasolevat küpsist teabega, et kasutaja on vastavat reklaami näinud. See tehnoloogia võimaldab koguda pika aja jooksul (on tuvastatud küpsiseid, mille kehtivus lõpeb aastal 9999) ja ulatuslikult teavet praktiliselt isiku kogu veebitegevuse kohta. Küpsiste kõrval kasutatakse jälgimiseks ka muid tehnoloogiaid, nt IP-aadressi, jälgimispiksleid ja ultrahelisignaale, mis võimaldavad lisaks külastatud veebisaitidele tuvastada kasutaja seadme asukoha füüsilises

maailmas, nt teatud kaupluse läheduses, mis saadab välja ultrahelisignaali, mida inimkõrv ei kuule, küll aga mobiiltelefoni mikrofon.

Reklaamitööstuses kasutatakse kõiki neid andmeid isikute profileerimiseks huvide, tutvusringkonna, päritolu, aadressi, vanuse ja muude tunnuste alusel ning seda teavet kasutatakse selleks, et kuvada kasutajale just neid reklaame, mis teda enim kõnetada ja tema ostukäitumist mõjutada võiksid. Käitumispõhise digireklaami kuvamisest on huvitatud nii veebisaidid, kes oma veebisaidil reklaamipinda välja üürivad ja sellega tulu teenivad (nt uudisteportaalid), kui ka oma toodete ja teenuste pakkujad ehk reklaamijad, kes nõnda sobivate klientideni jõuavad. St muuhulgas, et mitmesaja miljardiline reklaamiäri võimaldab paljudel veebisaitidel pakkuda kasutajatele internetis tasuta veebisisu. Õigusliku regulatsiooni muudatus, mis raskendab isikuandmete kättesaadavust ja töötlemist, olgu nõusoleku nõude või jälgimist keelavate vaikeseadete rakendamise näol, teeb suunatud reklaamil põhineva ärimudeli viljelemise väga keeruliseks. Arvestades ühelt poolt reklaamitööstuse osapoolte ja veebisaitide õigust ettevõtlusvabadusele ja teiselt poolt isikute õigust eraelu puutumatusele, on arusaadav, et menetletavas e-privaatsuse määruses võib kompromissi leidmine osutuda väga keeruliseks.

Teisele uurimisküsimusele vastamiseks uuriti küpsiste ja muude jälgimistehnoloogiate kasutamise regulatsiooni kehtivas e-privaatsuse direktiivis 2002/58/EÜ ning töö seisukohalt võtmetähtsusega sätte – artikli 5 lõike 3 – kujunemist. Artikli 5 lõige 3 käsitleb kasutaja lõppseadmesse teabe salvestamist ja juurdepääsu saamist sinna juba salvestatud teabele. 2002. aastal vastu võetud e-privaatsuse direktiivi menetlemisel kaaluti küpsise salvestamise lubatavuse aluseid, sh nõusolekut, kuid jäädi lõpuks loobumisvõimaluse (*opt out*) ja kasutaja teavitamise juurde. 2009. aastal võeti vastu e-privaatsuse direktiivi muudatused, millega mh kehtestati küpsise salvestamiseks eelneva nõusoleku nõue (*opt in*). Seejuures on kõnekas, et 13 liikmesriiki 22-st, nende seas Eesti, allkirjastas direktiivi muudatuste vastuvõtmisel seisukoha, milles deklareeriti sisuliselt, et senist artikli 5 lõikes 3 sätestatud loobumisvõimalust ei kavatseta muuta ja nõusolekut võib endiselt väljendada kasutaja teavitamise ja talle küpsistest loobumise võimaluse pakkumisega. See tähendab, et üle poole liikmesriikidest ei olnud tegelikult loobumisvõimaluselt nõustumisvõimalusele ülemineku poolt ega plaaninud seda jõustada, mis on üks põhjustest, miks kehtiva e-privaatsuse direktiivi ülevõtmine ja kohaldamine on olnud liikmesriikides niivõrd ebaühtlane.

Rääkides nõusolekust, on oluline märkida, et kehtiv e-privaatsuse direktiiv tugineb nõusoleku mõiste sisustamisel isikuandmete kaitse üldmäärusele (EL) 2016/679 (varasemalt selle eelkäijale andmekaitsedirektiivile 95/46/EÜ), mis tähendab, et küpsiste kasutamiseks antav nõusolek peab olema vabatahtlik, konkreetne, teadlik ja ühemõtteline tahteavaldus, mis on antud selge nõusolekut väljendava ehk aktiivse tegevusega. Küpsiste salvestamiseks aktiivse

tegevusega väljendatud nõusoleku nõuet on selgelt jaatanud ka Euroopa Liidu Kohus asjas *Planet49* tehtud lahendis. Muuhulgas sisaldasid e-privaatsuse direktiivi muudatused põhjenduspunkti, mille järgi võib nõusoleku anda ka rakenduse seadete kaudu, kui see vastab isikuandmete kaitse üldmääruse (varasemalt andmekaitsedirektiivi) tingimustele.

Kolmas uurimisküsimus puudutas menetluses oleva e-privaatsuse määruse peamisi vaidlusküsimusi seoses küpsiste ja muude jälgimistehnoloogiate reguleerimisega, millest käesolevas töös käsitleti viit probleemi. 2021. aasta veebruariks olid komisjon, parlament ja nõukogu kujundanud oma seisukohad, mille pinnalt alustada kolmepoolseid läbirääkimisi kompromisside leidmiseks ja e-privaatsuse määruse lõpliku teksti kinnitamiseks, mis andis hea võimaluse kõrvutada kõigi kolme institutsiooni positsioone omavahel ja õiguskirjanduses väljendatuga.

Esimene potentsiaalne vaidlusküsimus, mida uuriti, oli nõusoleku kui instituudi sobivus küpsiste kasutamise reguleerimiseks. Õiguskirjanduses on arutletud nn nõusoleku dilemma üle. See tähendab, et ühelt poolt soovitakse anda kasutajale otsustusõigus endaga seotud asjaolude, sh küpsiste lubamise või keelamise üle, teiselt poolt on teada, et keskmine veebikasutaja ei mõista küpsiste lubamisega kaasnevaid ohte ega selle toimepõhimõtteid – mida ei suuda alati mõista isegi valdkonna asjatundjad –, mis tähendab, et on väga raske tagada, et kasutaja nõusolek oleks teadlik. Küsimus on selles, kui palju otsustusi peaks riik üksikisiku eest tegema, et isikule jääks siiski tema autonoomia. Käesoleva töö autor leiab, et isiku vaba otsustusõiguse teostamisel on oluline lähtepunkt, millelt seda tegema asutakse. Autonoomiat on võimalik vabalt teostada nii küpsistest loobudes (*opt out*) kui ka küpsistega nõustudes (*opt in*).

Nõukogu on arutanud nõusoleku kõrval õigustatud huvile tuginemise võimaldamist, mida sooviksid reklaamitööstuse osapooled ja reklaamitulust sõltuvad veebisaidid, kuid komisjoni, parlamendi ja nõukogu seisukohad õigustatud huvile tuginemist ei luba. Ka käesoleva töö autor ei poolda uues e-privaatsuse määruses õigustatud huvi kui küpsiste kasutamise õigusliku aluse sätestamist, sest, nagu on selgitatud õiguskirjanduses, võib see kujuneda n-ö tagaukseks kõigi selliste töötlustoimingute tegemiseks, mida ühegi teise õigusliku alusega (nt nõusolek, teenuse osutamise erand) seadustada ei saa.

Teine probleemkoht, millele nii õiguskirjanduses kui ka EL-i enda institutsioonides tähelepanu juhitakse, on nõusoleku andmine rakenduse (nt veebisaidi, operatsioonisüsteemi) seadete kaudu. Komisjoni, parlamendi ja nõukogu seisukohad lubavad järeldada, et nõusoleku andmine rakenduse seadete kaudu saab uues e-privaatsuse määruses olema võimalik. Seda vaatamata seadete kaudu antava üldnõusoleku teoreetilistele probleemidele seoses sellise nõusoleku konkreetsuse, teadlikkuse ja vabatahtlikkusega. Rakenduse seadete kaudu antav nõusolek ei saa olla konkreetne ega teadlik isikuandmete kaitse üldmääruse järgi, kuna

üldnõusolek antakse etteulatuvalt nõustumise hetkel veel määratlemata või väga üldsõnaliste eesmärkide suhtes. Samuti ei saa üldnõusolek olla vabatahtlik, kuna vabatahtlikkus eeldab võimalust nõustuda iga üksiku eesmärgiga eraldi, mis ei pruugi veebilehitseja seadetes võimalik olla. Käesoleva töö autor nõustub siiski EL-i seadusandja seisukohaga lubada nõusoleku andmist rakenduse seadete kaudu, sest põhimõtteliselt ei ole keelatud võtta ühe õigusakti sätteid teise õigusakti üle ja neid vastavalt teise õigusakti vajadustele kohandada.

Kolmas ja üks kaalukamatest küsimustest on, millised saavad olema rakenduse vaikeseaded. Komisjoni, parlamendi ja nõukogu seisukohad lahknevad olulisel määral isikuandmete kaitse üldmäärusest tulenevate vaikimisi ja lõimitud andmekaitse põhimõtete rakendamise suhtes. Vaikimisi andmekaitse põhimõtte järgi peaksid rakenduse seaded olema enne kasutamist seadistatud küpsiseid ja muul viisil jälgimist keelama. Arvestades inimeste kalduvust säilitada olemasolev olukord (*status quo bias*), aitaksid privaatsust kaitsvad vaikeseaded tagada suurema hulga kasutajate eraelu puutumatuse kaitse. Lõimitud andmekaitse on oluline, sest see võimaldab n-ö alustada ahela algusest. Küpsiste kontekstis tähendab see, et küpsiste keelamiseks ja selle keelu jõustamiseks veebisaitide suhtes peavad veebilehitsejate tootjad rakendama sobivaid lahendusi ja privaatsust suurendavaid tehnoloogiaid juba toodete ja teenuste loomisel. Vastasel korral poleks kasutajal küpsiste keelamise õigusest suurt kasu.

Parlamendi seisukoht pakub kasutajale kõige suuremat kaitset, rakendades nii lõimitud kui ka vaikimisi andmekaitse põhimõtet. Parlamendi seisukoht näeb esiteks ette, et vaikimisi peab turule lastav tarkvara olema seadistatud kolmanda isiku poolt lõppseadmesse teabe salvestamist, selles oleva teabe töötlemist ja selle kohta teabe kogumist keelama. Teiseks sisaldub parlamendi seisukohas mitu sätet, milles pannakse tarkvaratootjatele siduvaid kohustusi privaatsuse tagamiseks teenustes ja toodetes. Komisjon rakendab lõimitud, kuid mitte vaikimisi andmekaitset, sätestades, et turule lastud tarkvara peab pakkuma võimalust keelata kolmandal isikul lõppkasutaja lõppseadmesse teabe salvestamine või juba lõppseadmesse salvestatud teabe töötlemine. Kahetsusväärselt ei sisalda nõukogu seisukoht ei vaikimisi ega lõimitud andmekaitse põhimõtet. Käesoleva töö autor leiab, et tõelise muutuse esilekutsumiseks on tarvis rakendada nii vaikimisi kui ka lõimitud andmekaitse põhimõtet.

Vaikimisi küpsiste keelamise vastu on selgelt reklaamitööstus ja reklaamitulust sõltuvad veebisaidid, nagu *online*-ajakirjandus, sest paljude veebisaitide jaoks on tasuta veebisisu esitamine võimalik vaid tänu veebisaidil oleva vaba reklaamipinna väljaüürimisele. Reklaamitööstus rõhutab, et kui kasutaja langetab otsuse juba veebilehitseja seadetes, võetakse ülejäänud osalistelt, sh kolmandatelt osapooltelt (nt andmevahendajalt, reklaamivõrgustikult) võimalus kasutajaga üldse dialoogi astuda, et temalt küpsise salvestamiseks nõusolekut küsida. Seda probleemi püütakse komisjoni, parlamendi ja nõukogu seisukohtades lahendada selliselt,

et isegi kui veebilehitseja on üldiselt seadistatud küpsiseid vaikimisi keelama, oleks konkreetsel veebisaidil õigus küsida kasutaja nõusolekut siis, kui kasutaja seda veebisaiti külastab.

Neljas vaieldav küsimus puudutab küpsisebarjääre, st olukorda, kus kasutajal pole võimalik veebisisuni jõuda, kui ta pole küpsistega nõustunud. Ühest küljest on küpsisebarjääri kasutamine vastuolus isikuandmete kaitse üldmääruses sätestatud nõusoleku vabatahtlikkusega, teiselt poolt piirab küpsisebarjääride keelamine veebisaitide ja rakenduse loojate ettevõtlusvabadust, eriti arvestades reklaamitulu olulisust nende tegevuses. Küpsisebarjääri keelustamise tõttu võivad teatud teenusepakkujad olla sunnitud tegevuse lõpetama, mille tõttu võib väheneda teenuste mitmekesisus ja konkurents, või jääb juurdepääs veebisisule nn maksumüüri (*pay walls*) taha, mis ei pruugi lõppastmes olla kasutajate huvides. Komisjoni ettepanekus küpsisebarjääre ei käsitleta, st komisjon toetab küpsisebarjääre nendest vaikimise teel. Parlament soovib küpsisebarjäärid keelata. Nõukogu soovib küpsisebarjäärid keelata teatud tingimustel, nt poolte selge ebavõrdsuse korral, st kui teenuse osutajal on domineeriv positsioon. Töö autor pooldab põhimõtteliselt nõukogu seisukohta, et teatud juhtudel peaksid küpsisebarjäärid olema keelatud, kuid leiab, et keelu rakendamise tingimused nõuavad täiendavat analüüsi.

Viiendaks on paljude huvirühmade jaoks tervitatav uues e-privaatsuse määruses sätestatav erand küpsiste kasutamiseks ilma kasutaja nõusolekuta, kui seda tehakse veebisaidi külastajate mõõtmiseks (nn statistiline või veebianalüütika erand). Komisjoni, parlamendi ja nõukogu seisukohad erinevad selles, kas ja millistel tingimustel võib veebisaidi omanik veebianalüütikateenuse tellida kolmandalt isikult. Komisjoni seisukoht lubab veebianalüütika erandi alusel küpsiste abil andmeid koguda ainult veebisaidil endal, mis ei arvesta väiksemate ettevõtete vajadusega seda teenust sisse osta. Parlamendi seisukoht lubab küpsistega kogutud andmeid kolmandale isikule edastada vaid kitsastes raamides, sh kohustades veebianalüütikateenuse pakkujat hoidma ühelt veebisaidilt saadud andmed eraldi teistelt veebisaitidelt saadud andmetest. Nõukogu seisukoht viitab andmete kolmandale isikule edastamisel isikuandmete kaitse üldmääruse vastutava ja volitatud töötleja regulatsioonile, kuid praktikas esineb oht, et veebianalüütikateenuse pakkuja kasutab veebisaidilt saadud andmeid siiski laiemalt reklaamitööstuse huvides isikute jälgimiseks.

Teine erand nõusoleku nõudest puudutab masinatevahelist sidet, mille näideteks on olukord, kus veebisaiti sisse kodeeritud ultrahelisignaal edastab läheduses olevale mikrofoniga seadmele teate, et kasutaja viibib parasjagu vastaval veebisaidil, või kus arukas külmkapp saadab reklaamivahendajale teavet kasutaja toitumisharjumuste kohta. Masinatevahelist sidet lubatakse ilma nõusolekuta edastada nii komisjoni, parlamendi kui ka nõukogu seisukohas sisuliselt vaid kasutaja teavitamise tingimusel. Parlament ja nõukogu sätestavad hilisema

andmete kustutamise või anonüümimise kohustuse. Käesoleva töö autor leiab, et kasutajal peaks alati olema võimalus isegi statistilisel eesmärgil andmekogumisest keelduda.

Kokkuvõttes võib öelda, et enamik komisjoni, parlamendi ja nõukogu seisukohtades välja pakutud lahendusi ei ole põhimõtteliselt uued ideed, vaid käesoleva töö autori arvates pigem varem tegemata jäänud töö. E-privaatsuse direktiivi kehtivuse ajal on korduvalt juhitud tähelepanu vajadusele kehtestada tarkvaratootjatele eraelu puutumatust kaitsvad siduvad nõuded, kuid need ei ole andnud tulemust. Käesoleva töö autor on veendunud, et kui tarkvara jälgimiskindlaks muutmine jääb taas tungiva soovituse tasandile uue e-privaatsuse määruse preambulis ilma siduva artiklita ja sätete üle järelevalve tegija määramiseta, ei ole põhjust suurt muutust oodata. Vaatamata paljudes veebilehitsejates küpsiste keelamise võimalusele, on paraku palju veebisaite, kes neid seadeid ja seega kasutajate soove ei austa, samuti tehnoloogiaid, mis suudavad kustutatud küpsised taasluua. Lõimitud andmekaitse põhimõtte rakendamine aitaks saavutada olukorra, kus andmekaitsereeglite rikkumine poleks mitte üksnes keelatud ja sanktsioneeritud, vaid ka tehniliselt takistatud.

Tulevikku vaadates tuleb arvestada ka uute jälgimise viisidega ja mitte takerduda üksnes küpsiste reguleerimisse. Käesoleva töö autor nõustub teatud huvirühmade seisukohaga, et uue e-privaatsuse määruse sõnastus peaks olema piisavalt avar, ent leiab, et printsiipidele lisaks oleks vaja luua õiguslik alus vajadusel neid printsiipe kohustatud isikutele siduvalt täpsustada. Eriti info- ja kommunikatsioonitehnoloogia valdkonnas on leitud, et lisaks üldisele lõimitud andmekaitse põhimõttele oleks vaja praktilisemat ja konkreetsemat lähenemist teatud kasutusjuhtudele suunatud eeskirjade näol.

Reklaamitööstuse ja selle eri osapoolte jaoks on kahjulikud mistahes meetmed, mis vähendavad nende ligipääsu andmetele, eeskätt aktiivse nõusoleku nõue, privaatsust kaitsvad vaikeseaded ja küpsisebarjääride keelustamine. Samas on õiguskirjanduses juhitud tähelepanu sellele, et käitumispõhine reklaam ei ole ainus reklaamimise viis. Kolmanda osapoole küpsiste vaikimisi keelamine ähvardab reklaamitööstuses levinud jälgimisel põhinevaid ärimudeleid, kuid mitte reklaamide esitamist veebis põhimõtteliselt. Oma tooteid ja teenuseid on võimalik turundada ka ilma isikute eraelu jälgimiseta. Lõppastmes ei ole küpsiste ja muude jälgimistehnoloogiate reguleerimine mitte õiguslik ega tehniline küsimus, vaid poliitiline väärtusküsimus. Ühiskonnad on ajaloo jooksul kuulutanud õigusvastaseks mitmesuguseid moraalselt vastuvõetamatuid tegevusi, nagu inimorganite, laste ja orjadega kaubitsemine. Asjaolu, et isikuandmetega kauplemise turg on olemas, ei tähenda, et selle peaks heaks kiitma seaduse tasandil. Käesoleva töö autor loodab, et eraelu puutumatuse kaitse ei ole Euroopas kümne-kahekümne aasta pärast samas või veel viletsamas seisus, vaid et suudame leida nõu ja jõu oma põhiväärtuste eest seista.

Regulation of Cookies and Similar Tracking Technologies in the European Union Data Protection Law. Summary

We are living in a world where every human being's every move is potentially covertly monitored and recorded, much like log files automatically record the processes of a computer program. This practice has been called life logging and such an order of society surveillance capitalism, which feeds on every experience of every human's life. This time the observer is not George Orwell's Big Brother, since at least in democratic countries, covert surveillance by public authorities is strictly regulated. Instead, the observer is the private sector, whose endeavours to develop ever new ways and technologies to amass, process, enrich with other data inventories and resell for profit yet a larger amount of data, have gone unchecked since the creation of the Internet at the beginning of the 1990s.

One of the best known and most widespread tracking technologies is the cookie, which was created in 1994, and is still the main driver of the digital advertising industry, which generates 300 billion dollars in global annual spending. However, during the 25 years since its creation, a myriad of similar tracking technologies have been developed and deployed in order to deliver targeted advertising. These technologies enable the tracker to identify the devices belonging to a user, the location of a user's device at any moment, websites visited by him, and ads he has seen or interacted with. This data is of great value to the advertising industry with its host of players, such as ad networks, data brokers, supply-side and demand-side platforms, and analytics providers, who collect and process data to create profiles of users. Ad networks serve as brokers between publishers, who wish to monetize the free space on their websites, and advertisers, who wish to target their ads at a specific audience.

While cookies and similar tracking technologies bring in a wealth of insights for the advertising industry, they are a potential threat to the privacy of the user. The European Consumer Commissioner noted in 2009 that the World Wide Web is becoming the World Wide West. In the face of these developments, the European Union (EU) has been reforming its data protection laws, including the e-privacy directive 2002/58/EC (ePD), which regulates the use of cookies and similar tracking technologies, among other things. At the time of writing this thesis, all three institutions involved in the EU legislation have formulated their positions to proceed with trilogue negotiations. The Commission proposed the new e-privacy regulation (ePR) in January 2017, the Parliament adopted its position in October 2017 and the Council reached a common position in February 2021.

This thesis addresses the problem of how to raise the level of privacy protection in the EU via the regulation of cookies and similar tracking technologies in the proposed ePR, while

at the same time accommodating the interests of the advertising industry as far as possible. The aim of the thesis is to propose ways to regulate cookies and similar tracking technologies so that the ePR would produce a change, allow for effective implementation, and protect the privacy of the user, while enabling data processing which inflicts little or no harm on users' privacy. The research questions posed in this thesis are as follows:

(1) What are cookies and similar tracking technologies and how can they threaten the privacy of individuals in the context of digital advertising?
(2) How have cookies and similar tracking technologies been regulated in the EU thus far and on which conditions is it allowed to collect data about web and smart device users via cookies and similar tracking technologies?
(3) What are the main issues in the proposed e-privacy regulation regarding the use of cookies and similar tracking technologies and how could they be solved?

The author uses the dogmatic method to answer these research questions since the principal objects of analysis are the legal acts in force and to be enforced in the future. The author aims to explain the significance of the selected provisions for the data subject and for the advertising industry. The findings will be presented following the order of the research questions.

In answer to the first research question, it was established that a cookie is an alphanumeric text file that a website stores on a user's computer to remember data related to the user, such as login details or items placed in the shopping basket in an online store. These are two examples of necessary cookies which allow the service to function properly. But there are also unnecessary cookies, such as analytics, preference and advertising cookies. When a user visits a website containing a number of ads (e.g. news site), his web browser sends requests to the servers hosting each ad in order to display them, and together with the ad, the server sends back a cookie and stores it on the user's computer or updates an existing cookie. This cookie contains the information that this user has now seen these particular adds. Cookies allow the tracker to collect data on the user's each move on the Internet and store it over a long period of time, e.g. researchers have discovered cookies set to expire in the year 9999. In addition to cookies, other tracking technologies include determining the location of a user in the physical world via his IP address, and using ultrasonic beacons at the entrance of a shop which emit ultrasonic signals inaudible for the human ear, but easily received by any device with a microphone.

The advertising industry relies on this information to build profiles of users' interests, acquaintances, ethnic origin, age, location, income etc, which are then used to target him with ads that are likely to nudge his purchasing behaviour. Apart from ad networks and advertisers,

digital advertising is an important source of income for website publishers, enabling them to offer free services and content to users. Loss of revenue from advertising might cause publishers to close down, deny access to the website unless users agree to cookies or require them to pay for content, which might not be in the interests of the user. In sum, this conflict of interests is one of the reasons why compromises in the proposed ePR will probably be hard to find in the trilogue negotiations.

The second research question concerned the applicable law at the time of writing this thesis regarding the use of cookies and similar tracking technologies. Firstly, it should be noted that the applicable ePD relies heavily on the terms and provisions of the General Data Protection Regulation (GDPR), and importantly for this thesis, the notion of consent. Article 5 paragraph 3 of the ePD initially only required the website to inform the user of the presence of cookies and to give him the right to refuse cookies. This is called the opt-out approach. In 2009, Article 5 paragraph 3 of the ePD was amended to require prior consent of the user before setting any cookies. This resulted in flooding the web with cookie notices and requests and the ePD being informally labeled the cookie law. This is called the opt-in approach. However, it appears from the procedural documents that 13 member states out of 22 signed a declaration essentially saying that they did not see the 2009 amendments as changing the previous opt-out regime and therefore did not intend to enforce it. As can be expected, this has resulted in a patchwork transposition of the 2009 amendments into national laws, and uneven enforcement.

In response to the third research question, five main issues were identified regarding the regulation of cookies and similar tracking technologies in the proposed ePR. The positions of the Commission, the Parliament and the Council were compared and analysed against the views expressed in the legal literature.

Firstly, the theoretical question of whether consent is an appropriate means to regulate the use of cookies and similar tracking technologies was studied. This relates to the so-called consent dilemma, whereby on the one hand, the user should be autonomous in deciding matters related to him, including allowing or prohibiting the use of cookies. However, an average web user is hardly capable of making informed decisions about cookies, since even many data protection professionals struggle to understand all the mechanisms involved in employing cookies in online marketing. On the other hand, the question is how far the state should go in protecting the individuals without unduly limiting their autonomy. The author of the thesis notes that the freedom to decide is related to an equally important question of what the starting position of exercising this right should be. It is possible to freely choose both by disabling cookies (opt out) and by accepting cookies (opt in). This has sparked perhaps the most heated debate surrounding the proposed ePR. As an alternative to consent, relying on the legitimate

interest of the processor (the person setting the cookie) has been suggested, but none of the legislative bodies of the EU supports it and neither does the author of the thesis.

The second problem discussed in the literature is whether consent can be given in the settings of an application (e.g. a website or an operating system). This idea is not new since it was included in the 2009 amendments to the ePD, though in the text of the preamble and not in a binding article. While it would be an appealing solution to the disruptive cookie banners, there are theoretical problems with giving consent via application settings. Such consent would run counter to the requirements of the GDPR, which defines valid consent as a freely given, specific, informed and unambiguous indication of the data subject's wishes. General consent expressed via settings cannot be specific and informed because at the time of consenting, the purposes and means of data processing and cookie setting may be undefined and too general. Neither can general consent be freely given as this entails the possibility to consent to each purpose separately, which might be hard to achieve in the settings of an application. The author of the thesis agrees with the EU legislative bodies that despite these discrepancies, consenting should be allowed in the application settings because in principle it is common practice to borrow terms from one legal act into another and change them to suit the purposes of the other act.

Thirdly, as mentioned above, the strongest opinions of stakeholders relate to the default settings of the application enabling the expression of consent. It is clear from the evidence of social studies that people are inclined to adhere to the default option (*status quo bias*), which would ensure privacy protection for a larger number of people. The privacy by default principle is closely tied to the privacy by design principle in the GDPR, which means that services and products must be created with user privacy in mind. An example of this is using end-to-end encryption in messaging apps.

While the EU legislative bodies agree on foreseeing the option of expressing consent in application settings, they are divided on what the default settings should be. The Parliament's position provides the most protection for a data subject. First, the Parliament requires software placed on the market to reject cookies and similar tracking technologies by default, and second, the Parliament's position imposes binding obligations on software producers not to weaken the level of protection. Therefore, the Parliament applies both privacy by default and privacy by design principles. The Commission would like to implement the privacy by design, but not the privacy by default principle, since it requires software producers to provide the option of refusing cookies and similar tracking technologies. The Council's position offers the least protection as it does not contain any provisions on these two principles. The author of this thesis

is of the opinion that fundamental change can only be achieved by applying both privacy by default and privacy by design principles.

As can be expected, the advertising industry, including websites depending on advertising revenue, opposes both the idea of giving consent in application settings and the requirement of privacy enhancing default settings. They argue that if the user can decide on allowing or disallowing cookies in the browser settings, all third parties would be deprived of direct access to users to even engage in a dialogue to obtain consent. This issue might be mitigated by enabling specific websites visited by the user to request user's consent even if his browser is set to prohibit the use of cookies.

The fourth problem concerns the quite common practice of denying access to content to users who block cookies (cookie walls). On the one hand, data protection activists argue that such consent cannot be considered freely given. On the other hand, this infringes on the websites' freedom to conduct business. It is doubtful whether the legislator can oblige businesses to offer their services freely, especially considering the importance of advertising revenue for many websites. It might mean simply replacing cookie walls with pay walls. The Parliament's position prohibits cookie walls, the Commission endorses them by omission. The Council wishes to make the ban on cookie walls dependent on, for instance, the dominant position of the website or service provider.

The fifth and last matter analysed in this thesis deals with exceptions to the consent rule. A welcome change to the existing ePD is the proposed exception for carrying out audience measurement, such as web analytics and statistics. All three legislative bodies of the EU support this exception, but they disagree on the conditions under which audience measurement can be outsourced from a third party. The Commission only makes the statistics exception for audience measurement conducted by the website or service provider itself, which does not meet the practical needs of smaller businesses who cannot afford an in-house IT department. The Parliament allows the website to transfer data to a third party for web analytics under strict terms, such as forbidding the third party to combine data from one website with data from another website. The Council in essence permits transfer to third parties under the conditions set forth in the GDPR regarding the provisions for data controller and data processor. The author of the thesis is concerned that in practice, such an exception might be taken advantage of in the interests of the advertising industry.

The second problematic exception relates to the use of machine-to-machine communications, such as the conveyance of ultrasonic signals between devices, and a smart refrigerator informing the ad network of its contents, and thus the eating habits of its owner. All three EU legislative bodies allow such communications without user's consent provided

that the user is notified of it. The Parliament and the Council foresee an obligation to anonymize data after its use. In the view of the author of this thesis, the user should always have the right to opt out of any, even merely statistical, data collection and processing.

In conclusion, most of the solutions contained in the positions of the Commission, the Parliament and the Council are not completely new, rather the author of the thesis finds that they represent issues previously left unaddressed. It has been repeatedly suggested over 20 years that software and hardware producers should be obligated to employ privacy enhancing technologies. These calls have gone unheeded by the industry. The author of this thesis is convinced that if the privacy by design principle continues to be a recommendation in the preamble of the ePR, there is little reason to expect fundamental change. Privacy by design would help to create a situation in which infringement of the right to privacy is not only prohibited and sanctioned, but also technically hindered. While it is true that any principle-based legal act is better suited to stand the test of time than an overly technical and detail-oriented legal act, the author of the thesis strongly supports authorizing certain bodies to co-ordinate or execute the creation of specific binding rules, such as technical standards for obtaining consent via application settings.

Any change in the regulatory landscape restricting access to data, be it by a prior consent requirement, default settings prohibiting the use of cookies or a ban on cookie walls, threatens the existence of business models depending on digital advertising. However, it has been noted that behavioural advertising is not the only method of advertising. Blocking third-party cookies by default threatens business models built on user tracking, but not advertising as such. It is possible to promote one's services and products without tracking the private lives of users. At the end of the day, the regulation of cookies and similar tracking technologies is not a legal or a technical issue, but a question of politics and values. Throughout history, societies have outlawed practices deemed to be morally unacceptable, such as trade in human organs, children and slaves. The fact that there is a market for personal data does not mean that it should be endorsed. The author of this thesis hopes that the state of privacy protection in the EU ten to twenty years from now will not be in a similar or worse condition, but that we will find the will and way to stand for our core values.

Kasutatud allikad

Kasutatud kirjandus

1. Adobe Analytics. – https://www.adobe.com/analytics/adobe-analytics.html# (17.02.2021).
2. All About Cookies. What information is in a cookie? (*sine anno*) – https://www.allaboutcookies.org/cookies/what-information-in-cookie.html (16.04.2021).
3. Alphabet Inc. Annual Report Pursuant to Section 13 or 15(D) of the Securities Exchange Act of 1934 for the Fiscal Year Ended December 31, 2019. – https://www.sec.gov/Archives/edgar/data/1652044/000165204420000008/goog10-k2019.htm#s7E164D6797425D368E0A2E18504CF241 (20.02.2021).
4. American Association of Political Consultants. Alexander P. Gage. (*sine anno*) – https://theaapc.org/about-us/board-of-directors/alex-gage/ (21.02.2021).
5. Amnesty International. Surveillance Giants: How the Business Model of Google and Facebook Threatens Human Rights. London: Amnesty International Ltd, 2019.
6. Angwin, J. The Web's New Gold Mine: Your Secrets. (30.07.2010) – The Wall Street Journal. https://news.tfionline.com/post/888296348/the-webs-new-gold-mine-your-secrets/amp; https://www.wsj.com/articles/SB10001424052748703940904575395073512989404 (16.02.2021).
7. Arp, D., Quiring, E., Wressnegger, C., Rieck, K. Privacy Threats through Ultrasonic Side Channels on Mobile Devices. – 2nd IEEE European Symposium on Security and Privacy. Paris: IEEE, 2017.
8. Article 29 Data Protection Working Party. Cookie Sweep Combined Analysis – Report. 14/EN, WP 229, 03.02.2015.
9. Article 29 Data Protection Working Party. Opinion 01/2012 on the data protection reform proposals. 00530/12/EN, WP 191, 23.03.2012.
10. Article 29 Data Protection Working Party. Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC). 17/EN, WP 247, 04.04.2017.
11. Article 29 Data Protection Working Party. Opinion 03/2016 on the evaluation and review of the ePrivacy Directive (2002/58/EC). 16/EN, WP 240. 19.07.2016.
12. Article 29 Data Protection Working Party. Opinion 04/2012 on Cookie Consent Exemption. 00879/12/EN, WP 194, 07.06.2012.

13. Article 29 Data Protection Working Party. Opinion 05/2014 on Anonymisation Techniques. 0829/14/EN, WP 216, 10.04.2014.
14. Article 29 Data Protection Working Party. Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC. 844/14/EN, WP 217, 09.04.2014.
15. Article 29 Data Protection Working Party. Opinion 1/2009 on the proposals amending Directive 2002/58/EC on privacy and electronic communications (e-Privacy Directive). 00350/09/EN, WP 159, 10.02.2009.
16. Article 29 Data Protection Working Party. Opinion 2/2010 on online behavioural advertising. 00909/10/EN, WP 171, 22.06.2010.
17. Article 29 Data Protection Working Party. Opinion 7/2000 on the European Commission Proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector of 12 July 2000 COM (2000) 385. 5042/00/EN/FINAL, WP 36, 02.11.2000.
18. Article 29 Data Protection Working Party. Opinion 8/2006 on the review of the regulatory Framework for Electronic Communications and Services, with focus on the ePrivacy Directive. 1611/06/EN, WP 126, 26.09.2006.
19. Article 29 Data Protection Working Party. Opinion 8/2014 on the on Recent Developments on the Internet of Things. 14/EN, WP 223, 16.09.2014.
20. Article 29 Data Protection Working Party. Recommendation 1/99 on Invisible and Automatic Processing of Personal Data on the Internet Performed by Software and Hardware. 5093/98/EN/final, WP 17, 23.02.1999.
21. Article 29 Data Protection Working Party. Recommendation 3/97 Anonymity on the Internet. XV D /5022/97 final, WP 6, 03.12.1997.
22. Article 29 Data Protection Working Party. The Future of Privacy. Joint contribution to the
Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data. 02356/09/EN, WP 168, 01.12.2009.
23. Article 29 Data Protection Working Party. Working Document 02/2013 providing guidance on obtaining consent for cookies. 1676/13/EN, WP 208, 02.10.2013.
24. Article 29 Data Protection Working. Opinion 02/2013 on apps on smart devices. 00461/13/EN, WP 202, 27.02.2013.
25. B10 NUMB3R5. The Database of Useful Biological Numbers. Average duration of a single eye blink. –

https://bionumbers.hms.harvard.edu/bionumber.aspx?&id=100706&ver=4 (22.02.2021).

26. Body of European Regulators for Electronic Communications (BEREC). Report on OTT services. BoR (16) 35, 2016.
27. Bond, R. The EU E-Privacy Directive and Consent to Cookies. – Business Lawyer (American Bar Association), Vol. 68, No. 1, 2012.
28. Brookman, J., Rouge, P., Alva, A., Yeung, C. Cross-Device Tracking: Measurement and Disclosures. – Proceedings on Privacy Enhancing Technologies 2017(2).
29. Böhm, W-T., Halim, V. Cookies zwischen ePrivacy und DS-GVO – was gilt? – MultiMedia und Recht, Heft 10, 2020.
30. Carter, L. M. Facebook video on 23.02.2021. – https://www.facebook.com/LisaCarter247/videos/10224788418206327/ (14.03.2021).
31. Commission nationale de l'informatique et des libertés. Complaint under article 82 loi N° 78-17 du 6 janvier 1978. – https://noyb.eu/sites/default/files/2021-04/AAIDcomplaint_Redacted.pdf (27.04.2021).
32. Commission of the European Communities. Communication from the Commission to the European Parliament and the Council. Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition – two years of application of the General Data Protection Regulation. COM(2020) 264 final. Brussels, 24.06.2020.
33. Commission of the European Communities. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. A European strategy for data. COM(2020) 66 final. Brussels, 19.02.2020.
34. Commission of the European Communities. Communication from the Commission to the European Parliament and the Council on Promoting Data Protection by Privacy Enhancing Technologies (PETs). COM(2007) 228 final. Brussels, 02.05.2007.
35. Commission of the European Communities. Report from the Commission. First report on the implementation of the Data Protection Directive (95/46/EC). COM(2003) 265 final. Brussels, 15.05.2003.
36. Competition and Markets Authority. Online platforms and digital advertising Market study final report. London, 2020.
37. Cookiebot. Cookie checker. Is your website GDPR and CCPA compliant? (01.04.2020) –https://www.cookiebot.com/en/cookie-checker/ (11.02.2021).
38. Cookiebot. GDPR and cookie consent. Compliant cookie use. (27.10.2020) – https://www.cookiebot.com/en/GDPR-cookies/ (17.02.2021).

39. Cookiebot. How do websites track users? Technologies and methods. GDPR Compliance. (*sine anno*) – https://cookiebot.dev/en/website-tracking/ (12.02.2021).
40. CookiePro. Website Tracking Technologies. (28.10.2020) – https://www.cookiepro.com/knowledge/website-tracking-technologies/ (12.02.2021).
41. CookiePro. What are Strictly Necessary Cookies? (11.12.2020) – https://www.cookiepro.com/knowledge/what-are-strictly-necessary-cookies/ (16.02.2021).
42. CookiePro. What is a Flash Cookie? (02.06.2020) – https://www.cookiepro.com/knowledge/what-is-a-flash-cookie/ (18.02.2021).
43. Corrigan, C. The Very Best Encrypted Messaging Apps. AVG. (26.03.2020 updated on 18.01.2021) – https://www.avg.com/en/signal/secure-message-apps (14.03.2021).
44. Council of Europe. European Commission for the Efficiency of Justice (CEPEJ). European Ethical Charter on the use of Artificial Intelligence in judicial systems and their environment. Adopted at the 31st plenary meeting of the CEPEJ. Strasbourg, 3–4 December 2018.
45. Council of the European Union. Adoption of the proposal for a Directive of the European Parliament and of the Council amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of electronic communications networks and services, and 2002/20/EC on the authorisation of electronic communications networks and services (LA + S) (third reading). Statements. Interinstitutional file: 2007/0247 (COD). 15864/09 ADD 1 REV 1. Brussels, 18.11.2009.
46. Council of the European Union. Common Position adopted by the Council on 28 January 2002 with a view to the adoption of the Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector. Interinstitutional File: 2000/0189 (COD). 15396/2/01 REV 2 ADD 1. Brussels, 29.01.2002.
47. Council of the European Union. Common position adopted by the Council on 16 February 2009 with a view to the adoption of a Directive of the European Parliament and of the Council amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on consumer protection cooperation. Interinstitutional File: 2007/0248 (COD). 16497/1/08 REV 1. Brussels, 16.02.2009.

48. Council of the European Union. Mandate for negotiations with EP on Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications). Interinstitutional File: 2017/0003(COD). 6087/21. Brussels, 10.02.2021.
49. Council of the European Union. Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications). Interinstitutional File: 2017/0003(COD). 6543/20. Brussels, 06.03.2020.
50. Craig, P., de Búrca, G. EU Law. Text, Cases, and Materials. Sixth ed. UK: Oxford University Press 2015.
51. Cyphers, B. Google's FLoC Is a Terrible Idea. – Electronic Frontier Foundation (03.03.2012) – https://www.eff.org/deeplinks/2021/03/googles-floc-terrible-idea (24.04.2021).
52. Debusseré, F. The EU E-Privacy Directive: A Monstrous Attempt to Starve the Cookie Monster. – International Journal of Law and Information Technology, Vol. 13, No. 1, 2005.
53. Deloitte. Evaluation and review of Directive 2002/58 on privacy and the electronic communication sector. Final Report. A study prepared for the European Commission DG Communications Networks, Content & Technology. EU, 2017.
54. Diemberger, C. Das datenschutzrechtliche Einwilligungserfordernis für den Einsatz von Identifikatoren zur Wiedererkennung von Internetnutzern im World Wide Web. Universität Wien, 2018.
55. Digital Guide Ionos. What are cookies? (05.06.20) – https://www.ionos.com/digitalguide/hosting/technical-matters/what-are-cookies/ (17.04.2021).
56. DLA piper UK LLP. Study on the revision of the ePrivacy Directive for ETNO (European Telecommunications Network Operator's Association). Brussels: DLA piper UK LLP, 2016.
57. Eesti Infotehnoloogia ja Telekommunikatsiooni Liit (ITL). Arvamus Euroopa Komisjoni poolt 10.01.2017. avaldatud e-privaatsuse määruse ettepaneku kohta. Esitatud Majandus- ja Kommunikatsiooniministeeriumile 02.02.2017.

58. van Eijk, R. J-W. Web Privacy Measurement in Real-Time Bidding Systems. A Graph-Based Approach to RTB system classification. Doctoral thesis. University of Leiden, 2019.
59. EKSS *sub vero* veebilehekülg. – https://www.eki.ee/dict/ekss/index.cgi?Q=veebilehek%C3%BClg&F=M (16.02.2021).
60. EKSS *sub vero* veebisait. – https://www.eki.ee/dict/ekss/index.cgi?Q=veebisait&F=M (16.02.2021).
61. Elcock, W. How to stop Google, Apple, and Microsoft from tracking your location. (07.08.2019) – https://www.comparitech.com/blog/vpn-privacy/stop-google-apple-microsoft-tracking-location/ (07.04.2021).
62. Englehardt, S., Narayanan A. Online Tracking: A 1-million-site Measurement and Analysis. – Computer Science Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security 2016.
63. E-teatmik *sub vero* access log. – http://vallaste.ee/ (16.04.2021).
64. E-teatmik *sub vero* cookie. – http://vallaste.ee/ (17.02.2021).
65. E-teatmik *sub vero* HTTP (HyperText Transfer Protocol). – http://vallaste.ee/ (16.02.2021).
66. E-teatmik *sub vero* HTTP header. – http://vallaste.ee/ (16.02.2021).
67. E-teatmik *sub vero* IP address. – http://vallaste.ee/ (17.04.2021).
68. E-teatmik *sub vero* open source (1). – http://vallaste.ee/ (07.03.2021).
69. E-teatmik *sub vero* state. – http://vallaste.ee/ (16.02.2021).
70. E-teatmik *sub vero* stateful. – http://vallaste.ee/ (16.02.2021).
71. E-teatmik *sub vero* stateless. – http://vallaste.ee/ (16.02.2021).
72. E-teatmik *sub vero* third party cookie. – http://vallaste.ee/ (16.02.2021).
73. E-teatmik *sub vero* URL (Uniform Resource Locator). – http://vallaste.ee/ (16.02.2021).
74. E-teatmik *sub vero* web beacon. – http://vallaste.ee/ (16.02.2021).
75. E-teatmik *sub vero* WWW (World Wide Web). – http://vallaste.ee/ (16.02.2021).
76. Euroopa Komisjon. Ettepanek: Euroopa Parlamendi ja nõukogu määrus, milles käsitletakse eraelu austamist ja isikuandmete kaitset elektroonilise side puhul ning millega tunnistatakse kehtetuks direktiiv 2002/58/EÜ (privaatsust ja elektroonilist sidet käsitlev määrus). COM(2017) 10 final, 2017/0003 (COD). Brüssel, 10.01.2017.
77. Euroopa Parlament. Raport ettepaneku kohta võtta vastu Euroopa Parlamendi ja nõukogu määrus, milles käsitletakse eraelu austamist ja isikuandmete kaitset elektroonilise side puhul ning millega tunnistatakse kehtetuks direktiiv 2002/58/EÜ

(privaatsust ja elektroonilist sidet käsitlev määrus). (COM(2017)0010 – C8-0009/2017 – 2017/0003(COD)), A8-0324/2017, 20.10.2017.

78. European Commission. Executive Summary of the Ex-post REFIT evaluation of the ePrivacy Directive Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on the protection of privacy and confidentiality in relation to electronic communications and repealing Directive 2002/58/EC („the ePrivacy Regulation"). SWD(2017) 6 final. Brussels, 10.01.2017.
79. European Commission. Impact Assessment Accompanying document to the Proposal for a Directive of the European Parliament and the Council amending European Parliament and Council Directives 2002/19/EC, 2002/20/EC and 202/21/EC; Proposal for a Directive of the European Parliament and the Council amending European Parliament and Council Directives 2002/22/EC and 2002/58/EC; Proposal for a Regulation of the European Parliament and the Council establishing the European Electronic Communications Markets Authority. SEC(2007) 1472. Brussels, 13.11.2007.
80. European Commission. Impact Assessment accompanying the document Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications). SWD(2017) 3 final. Part 1/3. Brussels, 10.01.2017.
81. European Commission. Impact Assessment accompanying the document Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications). SWD(2017) 3 final. Part 2/3. Brussels, 10.01.2017.
82. European Commission. Proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector. COM(2000) 385 final, 2000/0189(COD). OJ C 365 E, 19.12.2000, lk 223–229.
83. European Data Protection Board (EDPB). Guidelines 07/2020 on the concepts of controller and processor in the GDPR. Version 1.0. 02.09.2020.
84. European Data Protection Board (EDPB). Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications. Version 1.0. 28.01.2020.
85. European Data Protection Board (EDPB). Guidelines 4/2019 on Article 25 Data Protection by Design and by Default. Version 2.0. 20.10.2020.

86. European Data Protection Board (EDPB). Guidelines 8/2020 on the targeting of social media users. Version 1.0. 02.09.2020.
87. European Data Protection Board (EDPB). https://edpb.europa.eu/cookies_et (17.04.2021).
88. European Data Protection Board (EDPB). Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities. 12.03.2019.
89. European Data Protection Board (EDPB). Statement 03/2021 on the ePrivacy Regulation. 09.03.2021.
90. European Data Protection Board (EDPB). Statement of the EDPB on the revision of the ePrivacy Regulation and its impact on the protection of individuals with regard to the privacy and confidentiality of their communications. 25.03.2018.
91. European Data Protection Supervisor. Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content. 14.03.2017.
92. European Data Protection Supervisor. Opinion 5/2016. Preliminary EDPS Opinion on the review of the ePrivacy Directive (2002/58/EC). 22.07.2016.
93. European Data Protection Supervisor. Opinion 6/2017. EDPS Opinion on the Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation). 24.04.2017.
94. European Data Protection Supervisor. Opinion 7/2015. Meeting the challenges of big data. A call for transparency, user control, data protection by design and accountability. 19.11.2015.
95. European Data Protection Supervisor. Opinion of the European Data Protection Supervisor on the Proposal for a Directive of the European Parliament and of the Council amending, among others, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). – OJ C 181, 18.07.2008, lk 1–13.
96. European Data Protection Supervisor. Second opinion of the European Data Protection Supervisor on the review of Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). – OJ C 128, 06.06.2009, lk 28–41.

97. European Digital Rights (EDRi) and Cookiebot. Ad Tech Surveillance on the Public Sector Web. A special report on pervasive tracking of EU citizens on government and health service websites. *Sine loco*, 2019.
98. European Parliament legislative resolution of 24 September 2008 on the proposal for a directive of the European Parliament and of the Council amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on consumer protection cooperation (COM(2007)0698 – C6-0420/2007 – 2007/0248(COD)). Vastuvõetud tekst: P6_TC1-COD(2007)0248. – OJ C 8 E, 14.01.2010, lk 359–393.
99. European Union Agency for the Cooperation of Energy Regulators (ACER). EUROPA Analytics. (*sine anno*) – https://acer.europa.eu/Media/Pages/EUROPA-Analytics.aspx (17.04.2021).
100. Facebook Analytics. – https://analytics.facebook.com/ (17.02.2021).
101. Facebook, Inc. Annual Report Pursuant to Section 13 or 15(D) of the Securities Exchange Act of 1934 For the Fiscal Year Ended December 31, 2019. – https://www.sec.gov/Archives/edgar/data/1326801/000132680120000013/fb-12312019x10k.htm#s54AFD3C4F459576CAFAC623F7B94CED5 (20.02.2021).
102. Financial Express. How an Apple Watch possibly saved the life of this 58-year-old man. (05.02.2021) – https://www.financialexpress.com/industry/technology/how-an-apple-watch-possibly-saved-the-life-of-this-58-year-old-man/2188716/ (18.02.2021).
103. From, A. Cookie Consents and Notices under the EU Data Protection Framework. Master's Thesis. University of Helsinki, 2020.
104. Geradin, D., Katsifis, D. An EU competition law analysis of online display advertising in the programmatic age. – European Competition Journal, Vol. 15 No. 1, 2019.
105. González Guerrero, L. D. Control of Our Personal Data in the Big Data Era: The Case of Third Party Web Tracking. – Estudios Socio-Juridicos, Vol. 21, No. 1, January–June 2019.
106. Google Inc. Letter to United States Securities and Exchange Commission on 20.12.2013, Re: Form 10-K for the fiscal year ended December 31, 2012. – www.sec.gov/Archives/edgar/data/1288776/000128877613000074/filename1.htm (17.02.2021).
107. Google Marketing Platform. Analytics. – https://marketingplatform.google.com/about/analytics/ (17.02.2021).

108. Gordon, T. 10 Most Secure Messaging Apps – The Best Platforms & Solutions. (12.01.2021) – https://getstream.io/blog/most-secure-messaging-apps/ (14.03.2021).
109. Grimmelmann, J. Spyware vs. Spyware: Software Conflicts and User Autonomy. – Ohio State Technology Law Journal, Vol. 16, No. 1, Winter 2020.
110. Helberger, N., Zuiderveen Borgesius, F. J., Reyna, A. The Perfect Match? A Closer Look at the Relationship Between EU Consumer Law and Data Protection Law. – Common Market Law Review, Vol. 54, No. 5, 2017.
111. Hogan & Hartson LLP, Analysys Consulting Ltd. Preparing the next steps in regulation of electronic communications. A contribution to the review of the electronic communications regulatory framework. Final Report. July 2006.
112. Holton, K. Europe's new data law upends global online advertising. – Reuters 23.08.2018. – https://www.reuters.com/article/uk-advertising-gdpr-insight-idINKCN1L80HT (22.04.2021).
113. Hoofnagle, C. J., Soltani, A., Good, N., Wambach, D. J., Ayenson, M. D. Behavioral Advertising: The Offer You Cannot Refuse. – Harvard Law & Policy Review, Vol. 6, Issue 2, 2012.
114. Horne, K. 22 Top Website Analytics Tools To Grow Sales. (22.10.2020). – https://digital.com/web-analytics-software/ (24.04.2021).
115. Hotjar. Top 20 web analytics tools from our survey of 2000+ experts. (06.04.2021) – https://www.hotjar.com/web-analytics/tools/ (24.04.2021).
116. i-SCOOP. The new EU ePrivacy Regulation: what you need to know. (*sine anno*) – https://www.i-scoop.eu/GDPR/eu-eprivacy-regulation/ (28.03.2021).
117. Information Commissioner's Office (ICO). Big data, artificial intelligence, machine learning and data protection. Version 2.2. UK: ICO, 2017.
118. Information Commissioner's Office (ICO). Guidance on the use of cookies and similar technologies. Version 1.0.48. UK: ICO, 2019.
119. Information Commissioner's Office (ICO). Guide to the Privacy and Electronic Communications Regulations. Version 2.4.49. UK: ICO, 2018.
120. Interactive Advertising Bureau Europe (IAB). – https://www.iab.com/topics/privacy/ (21.02.2021).
121. Interactive Advertising Bureau Europe (IAB). Position on the proposal for an ePrivacy Regulation. (28.03.2017) – https://iabeurope.eu/knowledgehub/policy/iab-europe-position-paper-position-on-the-proposal-for-an-eprivacy-regulation/ (21.02.2021).

122. International Chamber of Commerce UK (ICC). Cookie guide Second ed. November 2012. – https://www.cookielaw.org/wp-content/uploads/2019/12/icc_uk_cookiesguide_revnov.pdf (11.02.2021).
123. Internet Engineering Task Force (IETF). HTTP State Management Mechanism. RFC 2109. February 1997. – https://tools.ietf.org/html/rfc2109 (16.02.2021).
124. Internet Engineering Task Force (IETF). HTTP State Management Mechanism. RFC 2965. October 2000. – https://tools.ietf.org/html/rfc2965 (16.02.2021).
125. Java T Point. Difference between Webpage and Website. (*sine anno*) – https://www.javatpoint.com/webpage-vs-website (16.02.2021).
126. Jones, M. L., Lee, J. Comparing Consent to Cookies: A Case for Protecting Non-Use. – Cornell International Law Journal, Vol. 53, No. 1, 2020.
127. Judson, B. To understand where the cookie is headed, let's look at its history. Digital Content Next. (16.11.2020) – https://digitalcontentnext.org/blog/2020/11/16/to-understand-where-the-cookie-is-headed-lets-look-at-its-history/ (16.02.2021).
128. Khandekar, C. Cookie Security and its Implementation in the Light of GD-PR and E-Privacy Regulation. Magistritöö. Tallinn University of Technology School of Information Technologies, 2019.
129. Kristol, D. M. HTTP Cookies: Standards, Privacy, and Politics. – ACM Transactions on Internet Technology, Vol. 1, No. 2, November 2001.
130. Krustok, I. Reaalajas reklaami ostmine. Gemius Estonia. (21.05.2015) – https://www.gemius.ee/468/reaalajas-reklaami-ostmine.html (22.02.2021).
131. Kuneva, M. Roundtable on Online Data Collection, Targeting and Profiling. SPEECH/09/156. Brussels, 31.03.2009. – https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_09_156 (16.03.2021).
132. Langhanke, C., Schmidt-Kessel, M. Consumer Data as Consideration. – Journal of European Consumer and Market Law, Heft 6, 2015.
133. Legislative Observatory. Procedure file 2017/0003(COD). Respect for private life and the protection of personal data in electronic communications. – https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2017/0003(COD)&l=en (26.03.2021).
134. Leszek, S. Electronic Marketing in the European Union and in the UK – Selected Issues. – International In-House Counsel Journal, Vol. 12, No. 49, Autumn 2019.
135. Markou, C. Behavioural Advertising and the New "EU Cookie Law" as a Victim of Business Resistance and a Lack of Official Determination. – Gutwirth, S., Leenes, R.,

De Hert, P. (koost). Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection. Netherlands: Springer, 2016.

136. Mattu, S., Hill, K. Facebook Knows How to Track You Using the Dust on Your Camera Lens. (01.11.2018) – https://gizmodo.com/facebook-knows-how-to-track-you-using-the-dust-on-your-1821030620 (09.04.2021).
137. MDN Web Docs. Mozilla. What is the difference between webpage, website, web server, and search engine? (*sine anno*) – https://developer.mozilla.org/en-US/docs/Learn/Common_questions/Pages_sites_servers_and_search_engines (16.02.2021).
138. Mihaildis, A, Colonna, L. A Methodological Approach to Privacy by Design within the Context of Lifelogging Technologies. – Rutgers Computer and Technology Law Journal, Vol. 46, No. 1, 2020.
139. Mozilla position paper on the European Commission's draft e-Privacy Regulation. 2017. – https://blog.mozilla.org/netpolicy/files/2017/10/ePrivacy-position-paper-_-FINAL.pdf (23.04.2021).
140. Nield, D., Turner, B. Best encrypted instant messaging apps of 2021 for Android. (13.01.2021) – https://www.techradar.com/best/best-encrypted-messaging-app-android (14.03.2021).
141. NOYB. 101 Complaints on EU-US transfers filed. (17.08.2020) – https://noyb.eu/en/101-complaints-eu-us-transfers-filed (27.04.2021).
142. O'Driscoll, A. How ultrasonic tracking apps may be listening to you and how to block them. (18.10.2019) – https://www.comparitech.com/blog/information-security/block-ultrasonic-tracking-apps/ (17.02.2021).
143. OECD. Artificial Intelligence in Society. Paris: OECD Publishing, 2019.
144. Popper, J. jt. Artificial intelligence across industries. White Paper. Geneva: International Electrotechnical Commission, 2018.
145. Privacy International. How Apps on Android Share Data with Facebook (even if you don't have a Facebook account). 2018.
146. Ramirez, E. jt. Data Brokers: A Call for Transparency and Accountability. USA: Federal Trade Commission, 2014.
147. Randlo, T. Google katsetab uut kasutajate jälgimise viisi: kontrolli, kas oled testrühmas. – Postimees 14.04.2021. – https://majandus24.postimees.ee/7225007/google-katsetab-uut-kasutajate-jalgimise-viisi-kontrolli-kas-oled-testruhmas?_ga=2.73232659.1814441037.1618472410-1340925722.1567145559 (15.04.2021).

148. Rothenberg, R. Has Mozilla Lost its Values? (16.07.2013) – https://www.iab.com/news/has-mozilla-lost-its-values/ (22.04.2021).
149. Scherb, M. Free Content's Future: Advertising, Technology, and Copyright. – Northwestern University Law Review, Vol. 98, No. 4, 2004.
150. Schneier, B. The Eternal Value of Privacy. (18.05.2006) – https://www.schneier.com/essays/archives/2006/05/the_eternal_value_of.html (17.02.2021).
151. Sears, A. M. The Limits of Online Price Discrimination in Europe. – Columbia Science and Technology Law Review, Vol. 21, No. 1, Fall 2019.
152. Sherman, F. What Does Advertising-Supported Revenue Model Mean? Small Business. Chron. (08.12.2020) – https://smallbusiness.chron.com/advertisingsupported-revenue-model-mean-63332.html (23.02.2021).
153. SilverPush. – https://www.silverpush.co/ (17.02.2021).
154. Solove, D. J. Introduction: Privacy Self-Management and the Consent Dilemma. – Harvard Law Review, Vol. 126, No. 7, 2013.
155. Specht, L., Kerber, W. Datenrechte – Eine Rechts- und Sozialwissenschaftliche Analyse im Vergleich Deutschland – USA. Germany: ABIDA, 2018.
156. Spindler, G. Klarheit für Cookies. – Neue Juristische Wochenschrift, Heft 35, 2020.
157. Stack Overflow. Set a cookie to never expire. (*ca* 2010) – https://stackoverflow.com/questions/3290424/set-a-cookie-to-never-expire (20.02.2021).
158. Sullivan, J. Personalization with Respect. (10.05.2013) – https://blog.mozilla.org/blog/2013/05/10/personalization-with-respect/ (22.04.2021).
159. Sweeney, M. What Is a Demand-Side Platform (DSP) and How Does It Work? The Clearcode Blog. (27.11.2020) – https://clearcode.cc/blog/demand-side-platform/ (22.02.2021).
160. Zanfir-Fortuna, G. Will the ePrivacy Reg overshadow the GDPR in the age of IoT? International Association of Privacy Professionals. (16.02.2017) – https://iapp.org/news/a/will-the-eprivacy-reg-overshadow-the-GDPR-in-the-age-of-iot/ (07.04.2021).
161. Zawadziński, M. What is a Data Management Platform (DMP) and How Does it Work? The Clearcode Blog. (27.11.2020) – https://clearcode.cc/blog/data-management-platforms/ (22.02.2021).

162. Zawadziński, M. What Is an Ad Network and How Does It Work? The Clearcode Blog. (20.20.2021) – https://clearcode.cc/blog/what-is-an-ad-network-and-how-does-it-work/ (22.02.2021).
163. Zawadziński, M., Wlosik, M. What Is a Supply-side Platform (SSP) and How Does It Work? The Clearcode Blog. (25.11.2020) – https://clearcode.cc/blog/what-is-supply-side-platform/ (22.02.2021).
164. Zuboff, S. The Age of Surveillance Capitalism. The Fight for a Human Future at the New Frontier of Power. USA: Public Affairs, Hachette Book Group, 2019.
165. Zuboff, S. You Are Now Remotely Controlled. Surveillance capitalists control the science and the scientists, the secrets and the truth. – The New York Times 24.01.2020. – https://www.nytimes.com/2020/01/24/opinion/sunday/surveillance-capitalism.html (14.02.2021).
166. Zuiderveen Borgesius, F. J. Informed Consent: We Can Do Better to Defend Privacy. IEEE Security & Privacy. Vol. 13, No. 2, March / April 2015.
167. Zuiderveen Borgesius, F. J. Personal data processing for behavioural targeting: which legal basis? – International Data Privacy Law, Vol. 5, No. 3, 2015.
168. Zuiderveen Borgesius, F. J., Kruikemeier, S. jt. Tracking Walls, Take-It-Or-Leave-It Choices, the GDPR, and the ePrivacy Regulation. – European Data Protection Law Review, Vol. 3, No. 3, 2017.
169. Zuiderveen Borgesius, F. J., Steenbruggen, W. The Right to Communications Confidentiality in Europe: Protecting Privacy, Freedom of Expression, and Trust. – Theoretical Inquiries in Law, Vol. 20, Issue 1, January 2019.
170. Tartu Ülikool, arvutiteaduse instituut. Õppeaine Infoturve (MTAT.07.028). Privaatsus ja anonüümsus veebis – https://courses.cs.ut.ee/2018/infsec/spring/Main/Loeng-Anon%C3%BC%C3%BCmsusVeebis (17.02.2021).
171. Tene, O., Polonetsky, J. To Track or "Do Not Track": Advancing Transparency and Individual Control in Online Behavioral Advertising. Minnesota Journal of Law, Science & Technology, Vol. 13, No. 1, 2012.
172. Thaler, R. H., Sunstein, C. R. Nudge: Improving Decisions About Health Wealth And Happiness. New Haven: Yale University Press, 2008.
173. United States Senate, Committee on Commerce, Science, and Transportation. Office of Oversight and Investigations Majority Staff. A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes. Staff Report for Chairman Rockefeller. (18.12.2013) – https://www.govinfo.gov/content/pkg/CHRG-113shrg95838/html/CHRG-113shrg95838.htm (16.03.2021).

174. Urban, T., Degeling, M., Holz, T., Pohlmann, N. Beyond the Front Page: Measuring Third Party Dynamics in the Field. – WWW '20: Proceedings of The Web Conference 2020.
175. Vikipeedia, *sub vero* HTTP-küpsis. – https://et.wikipedia.org/wiki/HTTP-k%C3%BCpsis (17.02.2021).
176. Vladeck, D. C. Consumer Protection in an Era of Big Data Analytics. – Ohio Northern University Law Review, Vol. 42, No. 2, 2016.
177. Wikipedia *sub vero* HTTP cookie. – https://en.wikipedia.org/wiki/HTTP_cookie (16.02.2021).
178. Wikipedia *sub vero* Hypertext Transfer Protocol. – https://en.wikipedia.org/wiki/Hypertext_Transfer_Protocol (16.02.2021).
179. Wikipedia *sub vero* Web server. – https://en.wikipedia.org/wiki/Web_server (16.02.2021).
180. Wikipedia *sub vero* World Wide Web. – https://en.wikipedia.org/wiki/World_Wide_Web (16.02.2021).
181. World Wide Web Consortium. – https://www.w3.org/Consortium/ (07.04.2021).
182. World Wide Web Consortium. Tracking Compliance and Scope. W3C Working Group Note 22 January 2019. – https://www.w3.org/TR/tracking-compliance/ (07.04.2021).

Kasutatud õigusaktid

183. 11. detsembri 2018. aasta Euroopa Parlamendi ja nõukogu direktiiv (EL) 2018/1972, millega kehtestatakse Euroopa elektroonilise side seadustik. – ELT L 321, 17.12.2018, lk 36–214.
184. 12. juuli 2002. aasta Euroopa Parlamendi ja nõukogu direktiiv 2002/58/EÜ, milles käsitletakse isikuandmete töötlemist ja eraelu puutumatuse kaitset elektroonilise side sektoris (eraelu puutumatust ja elektroonilist sidet käsitlev direktiiv). – EÜT L 201, lk 37–47 (eestikeelne eriväljaanne: ptk 13, kd 29, lk 514–524).
185. 24. oktoobri 1995. aasta Euroopa Parlamendi ja nõukogu direktiiv 95/46/EÜ üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta. – EÜT L 281, 23.11.1995, lk 31–50 (eestikeelne eriväljaanne: ptk 13 kd 15, lk 355–374).
186. 25. novembri 2009. aasta Euroopa Parlamendi ja nõukogu direktiiv 2009/136/EÜ, millega muudetakse direktiivi 2002/22/EÜ universaalteenuse ning kasutajate õiguste kohta elektrooniliste sidevõrkude ja -teenuste puhul, direktiivi 2002/58/EÜ, milles

käsitletakse isikuandmete töötlemist ja eraelu puutumatuse kaitset elektroonilise side sektoris, ning määrust (EÜ) nr 2006/2004 tarbijakaitseseaduse jõustamise eest vastutavate siseriiklike asutuste vahelise koostöö kohta. – ELT L 337, lk 11–36.

187. 27. aprilli 2016. aasta Euroopa Parlamendi ja nõukogu määrus (EL) 2016/679 füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus). – ELT L 119, 04.05.2016, lk 1–88.
188. märtsi 2002. aasta Euroopa Parlamendi ja nõukogu direktiiv 2002/21/EÜ elektrooniliste sidevõrkude ja -teenuste ühise reguleeriva raamistiku kohta (raamdirektiiv). – EÜT L 108, 24.04.2002, lk 33–50 (eestikeelne eriväljaanne: ptk 13, kd 29, lk 349–366).
189. 9. märtsi 1999. aasta Euroopa Parlamendi ja nõukogu direktiiv 1999/5/EÜ raadioseadmete ja telekommunikatsioonivõrgu lõppseadmete ning nende nõuetekohasuse vastastikuse tunnustamise kohta. – EÜT L 91, 07.04.1999, lk 10–28 (eestikeelne eriväljaanne: ptk 13 kd 23 lk 254–272).
190. Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector. – OJ L 24, 30.01.1998, lk 1–8.
191. Euroopa Liidu lepingu konsolideeritud versioon. – ELT C 326, 26.10.2012, lk 13–390.

Kasutatud kohtupraktika

192. EKo C-311/18, *Data Protection Commissioner* versus *Facebook Ireland Ltd*, *Maximillian Schrems*, ECLI:EU:C:2020:559.
193. EKo C-362/14, *Maximillian Schrems* versus *Data Protection Commissioner*, ECLI:EU:C:2015:650.
194. EKo C-40/17, *Fashion ID GmbH & Co. KG* versus *Verbraucherzentrale NRW eV*, ECLI:EU:C:2019:629.
195. EKo C-673/17, *Planet49 GmbH* versus *Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV*, ECLI:EU:C:2019:801.
196. Liidetud kohtuasjad EKo C-203/15 ja C-698/15, *Tele2 Sverige AB* versus *Post- och telestyrelsen ning Secretary of State for the Home Department versus Tom Watson jt*, ECLI:EU:C:2016:970.

197. Liidetud kohtuasjad EKo C-293/12 ja C-594/12, *Digital Rights Ireland Ltd* versus *Minister for Communications, Marine and Natural Resources jt* ning *Kärntner Landesregierung jt*, ECLI:EU:C:2014:238.
198. *University of London Press Ltd* v *University Tutorial Press Ltd. Chancery Division*, [1916] 7 WLUK 79.