

**TALLINNA TEHNIKAÜLIKOOL**

Majandusteaduskond

Õiguse instituut

Heiko Jets

**ISIKUANDMETE AVALDAMISE ÕIGUSLIK REGULATSIOON  
ANDMETE AVALDAMISE KONTEKSTIS AUTO  
PARDAKAAMERATE NÄITEL**

Bakalaureusetöö

Juhendaja: Kärt Salumaa, MA

Tallinn 2017

Deklareerin, et käesolev bakalaureusetöö,  
mis on minu iseseisva töö tulemus, on  
esitatud Tallinna Tehnikaülikooli  
bakalaureusekraadi taotlemiseks ja selle  
alusel ei ole varem taotletud akadeemilist  
kraadi.

Heiko Jets

02.05.2017

Töö vastab kehtivatele nõuetele

Kärt Salumaa, MA

02.05.2017

/allkirjastatud digitaalselt/

Kaitsmisele lubatud "....." 2017

Õiguse instituudi bakalaureusetööde kaitsmiskomisjoni esimees

## Sisukord

<b>Sissejuhatus .....</b>	<b>5</b>
<b>1. Pardakaamera salvestise avaldamise õiguslik raamistik ja vastutus .....</b>	<b>7</b>
<b>1.1 Isikuandmete kaitse õiguslik raamistik Eestis .....</b>	<b>7</b>
<b>1.2 Isikuandmete kaitse õiguslik raamistik Euroopas .....</b>	<b>9</b>
<b>1.3 Salvestamine isiklikuks otstarbeks .....</b>	<b>11</b>
<b>1.4 Salvestise avaldamine .....</b>	<b>13</b>
1.4.1 Juhud, kus isikuandmete avaldamine on lubatud .....	14
1.4.1.1 Andmesubjekti nõusolek .....	14
1.4.1.2 Ajakirjanduslik eesmärk ja avalik huvi .....	16
1.4.1.3 Avaldamine asutusele, kes töötleb isikuandmeid seaduses sätestatud ülesande täitmiseks .....	20
1.4.1.4 Avaldamise eesmärgil salvestamine .....	20
1.4.2 Juhud, kus isikuandmete avaldamine on keelatud .....	21
1.4.2.1 Andmesubjekt äratuntav ja nõusolek puudub .....	21
<b>1.5 Isiku tuvastamine .....</b>	<b>23</b>
1.5.1 Isiku kaudne tuvastamine .....	23
1.5.2 Isiku otsene tuvastamine .....	25
<b>1.6 Vastutus .....</b>	<b>26</b>
1.6.1 Vastutust välistavad asjaolud .....	26
1.6.2 Haldusvastutus .....	28
1.6.3 Tsiviilvastutus .....	31
<b>2. Auto pardakaameratele ja isikuandmete töötlemiseolukordadele kehtiva õigusraamistiku tulevik .....</b>	<b>34</b>
<b>Kokkuvõte .....</b>	<b>38</b>
<b>Legal Regulation of the Publication of Personal Data in the Context of Publishing Data on the Example of Car Onboard Cameras .....</b>	<b>41</b>
<b>Kasutatud allikate loetelu .....</b>	<b>44</b>

## Lühendid

AKI	Andmekaitse Inspeksioon
EIKo	Euroopa Inimõiguste Kohtu otsus
EKo	Euroopa Kohtu otsus
HMS	Haldusmenetluse seadus
IKS	Isikuandmete kaitse seadus
KorS	Korraldusseadus
PS	Eesti Vabariigi põhiseadus
RKHKo	Riigikohtu halduskolleegiumi otsus
RKTKo	Riigikohtu tsiviilkolleegiumi otsus
RKÜKo	Riigikohtu üldkogu otsus
VÕS	Võlaõigusseadus

## Sissejuhatus

Tehnoloogia kiire areng paneb inimesed üha enam mõtlema oma privaatsusele. Internet ja erinevad sotsiaalmeedia kanalid võimaldavad inimestel kiiresti infot vahetada ning kõiksugused salvestavad seadmed, nagu näiteks kaamerad, muutuvad üha väiksemaks, taskukohasemaks ning inimestele kättesaadavamaks. Privaatsuse küsimus kaasneb ka esmapilgul ohutuna ja tavapärasesena tunduvate tegevustega nagu näiteks viibides avalikus kohas erinevate kaamerate vaateväljas, teostades otsingumootoris otsingut, broneerides reisi, makstes internetipangas arveid või isegi laenutades raamatukogust raamatut<sup>1</sup>.

Eestis ja ka mujal maailmas on üha populaarsemaks muutunud autole pardakaamerate paigaldamine, et vältida võimalikke vaidlusi õnnetusjuhtumi korral<sup>2</sup> või lihtsalt midagi huvitavat salvestada. Uuringute kohaselt laieneb pardakaamerate turuosa ülemaailmselt aastatel 2015-2022 17,4% aastas<sup>3</sup>. Ühtlasi meeldib inimestele oma videoid jagada kas erinevates videokeskkondades või sotsiaalmeedias, kui midagi põnevat on kaadrisse jäänud. Olenevalt video sisust võib see osutada üsna populaarseks. Ei mõelda aga sellele, mis vastavale videole võib olla veel peale jäänud ja et sellega võidakse rikkuda kellegi õigusi ning minna vastuollu eelkõige isikuandmete kaitse seadusega. Kuna sotsiaalmeedias võib kohata sarnaseid videoid üha enam, siis väärib ka teema kajastamist.

Töö eesmärk on uurida, millistel juhtudel võib füüsiline isik videomaterjali avaldada ning millistel juhtudel tuleb olla avaldamisel ettevaatlik, kuna võib avaldamisega rikkuda kellegi õigusi ning teda võidakse võtta vastutusele. Ühtlasi üritab töö heita pilgu tulevikku ja arutleda, kus suunas võiks auto pardakaamerate videote avaldamise regulatsioon liikuda.

2015. aastal registreeris Andmekaitse Inspeksioon (AKI) oma infotelefonis 147 isikuandmete Internetis avaldamise (avaldamise lõpetamise) küsimust<sup>4</sup>, mis moodustab ligi 13% kõikidest

---

<sup>1</sup> Rengel, A. Privacy-Invasive Technologies and Recommendations for Designing a Better Future for Privacy Rights. *Intercultural Human Rights Law Review*, 2013, Vol. 8, lk 179.

<sup>2</sup> Postimees. Autokaamerad aitavad kindlustusel lahendada mitmeid juhtumeid kuus, 2016. [tarbija24.postimees.ee/3960039/autokaamerad-aitavad-kindlustusel-lahendada-mitmeid-juhtumeid-kuus](http://tarbija24.postimees.ee/3960039/autokaamerad-aitavad-kindlustusel-lahendada-mitmeid-juhtumeid-kuus) (28.04.2017).

<sup>3</sup> Credence Research, The Global Dashcams Market to Reach US\$ 5,530.0 Mn by 2022, 2016. [www.credenceresearch.com/press/the-global-dashcams-market](http://www.credenceresearch.com/press/the-global-dashcams-market) (03.04.2017).

<sup>4</sup> Andmekaitse Inspeksioon. Avaliku teabe seaduse ja isikuandmete kaitse seaduse täitmisest aastal 2015. Soovitused aastaks 2016, 2016. [www.aki.ee/sites/www.aki.ee/files/elfinder/article\\_files/AASTARAAMAT.pdf](http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/AASTARAAMAT.pdf) (05.03.2017), lk 6.

päringutest (kokku 1136 kõne). See tähendab, et AKIs oli päevakorral Internetis avaldamise ja avaldamise lõpetamise küsimus keskmiselt igal teisel tööpäeval. 2016. aastal suurenes üldine päringute arv ligikaudu 4%, ehk kokku oli kõnesid 1419<sup>5</sup>. Konkreetselt isikuandmete avaldamise ja avaldamise lõpetamise küsimusi esitati 204 korral<sup>6</sup>, mis moodustab kõikidest päringutest veidi üle 14%. Kui protsentuaalne vahe võrreldes 2015. aastaga ei ole suur, siis arvestades, et 2016. aastal oli 255 tööpäeva, tuli keskmiselt AKI-l tegeleda küsimusega pea iga päev. Nende andmete põhjal ei saa autor väita, et trend on selgelt kasvav, kuid see näitab, et küsimus on päevakajaline ja vajab teadlikkuse tõstmiseks käsitlemist.

**Bakalaureusetöö hüpotees on, et füüsilise isiku isiklikuks otstarbeks salvestatud auto pardakaamera video avaldamine võib kaasa tuua vastutuse. Töö uurimisküsimus on, millised on isiklikuks otstarbeks salvestatud auto pardakaamera salvestise avaldamise võimalikud tagajärjed füüsilisest isikust avaldajale.**

Töö esimese peatükis kirjutab autor isikuandmete avaldamise õiguslikust raamistikust Eestis kui ka Euroopas. Lisaks analüüsib autor, millistel juhtudel on isikuandmeid sisaldava salvestise avaldamine lubatud ja millistel keelatud, millised on isiku tuvastamise alused ning vastutus, kui andmesubjekti õigusi on rikutud.

Teises peatükis analüüsib autor, milline võiks olla auto pardakaamerate ja neile kehtivate reeglite tulevik.

Töös kasutatakse peamiselt dogmaatilist ja analüütilist meetodit, mis võimaldavad mõista isikuandmete kaitse kujunemislugu, hetkeseisu ja tulevikuvaateid antud valdkonnas.

Autor tugineb bakalaureusetöö kirjutamisel peamiselt nii rahvusvaheliste kui Eesti isikuandmeid ja nende avaldamist puudutavatele teadusartiklitele, kuna pidevas muutumises olevas valdkonnas pakuvad just need adekvaatsemat sisu. Suures osas kasutab autor lisaks AKI artikleid, aastaraamatuid ja soovitusi, kuna just AKI on see asutus, kes teostab andmekaitse nõuete täitmise üle järelevalvet ning selles valdkonnas teavitustööga aktiivselt tegeleb.

---

<sup>5</sup> Andmekaitse Inspeksioon. Avaliku teabe seaduse ja isikuandmete kaitse seaduse täitmisest 2016. aastal. Soovitused aastaks 2017, 2017. [www.aki.ee/sites/www.aki.ee/files/elfinder/article\\_files/aastaraamat\\_2016.pdf](http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/aastaraamat_2016.pdf) (22.04.2017), lk 7.

<sup>6</sup> Kuna AKI aastaraamatus ei olnud eraldi antud statistikat välja toodud, siis tegi autor AKI-sse selgitustaotluse ning 24.04.2017 täpsustas AKI vastavat statistikat.

# 1. Pardakaamera salvestise avaldamise õiguslik raamistik ja vastutus

## 1.1 Isikuandmete kaitse õiguslik raamistik Eestis

Eesti Vabariigi põhiseaduse<sup>7</sup> (PS) § 19 järgi on igaühel õigus vabale eneseteostusele ning igaüks peab oma õiguste ja vabaduste kasutamisel ning kohustuste täitmisel austama ja arvestama teiste inimeste õigusi ja vabadusi ning järgima seadust. PS isikuandmete kaitse on tuletatav õigusest informatsioonilisele enesemääramisele ja õigusest eraelu puutumatusel<sup>8</sup>. PS kommenteeritud väljaande mõistes on õigus informatsioonilisele enesemääramisele isiku õigus ise otsustada, kas ja kui palju isiku kohta enda kohta andmeid kogutakse ja salvestatakse<sup>9</sup>. Ühtlasi peab olema isikul õigus ise enda kohta käivate andmete avaldamise üle otsustada, kas ja millisel viisil ta tahab end avalikult kujutada ning mil määral tohivad teised teda muuta avaliku arutelu osaliseks<sup>10</sup>.

Isikuandmetele pakub kaitset ka PS § 26, mis sätestab, et igaühel on õigus eraelu puutumatusel<sup>11</sup>. Riigikohus on leidnud, et eraelu kaitse üheks oluliseks valdkonnaks on isikuandmete kaitse ning selle puutumatus riiveks on ka isikuandmete kogumine, säilitamine, kasutamine ja avaldamine sõltumata nende vormist<sup>12</sup>. Samale seisukohale on jäänud Euroopa Kohus<sup>13</sup>.

Eestis reguleerib isikuandmetega seonduvat valdkonda peamise õigusaktina isikuandmete kaitse seadus<sup>14</sup> (IKS). IKS-i eesmärk on kaitsta isikuandmete töötlemisel füüsilise isiku põhiõigusi ja -vabadusi, eelkõige õigust eraelu puutumatusel<sup>15</sup>. See tähendab, et eraelu alla kuuluvad ka suhted teiste isikutega ja isikutevahelised kontaktid<sup>16</sup>. IKS § 4 lg 1 defineerib isikuandmeid kui mis tahes andmeid tuvastatud või tuvastamata füüsilise isiku kohta ning nende vorm ei ole oluline. See tähendab, et näiteks isegi isiku kujutis liigitub isikuandmete alla,<sup>17</sup> kui seda kujutist on

---

<sup>7</sup> PS RT I, 15.05.2015, 2.

<sup>8</sup> Kungas, M. Traditsiooniliste õiguskaitsevahendite rakendatavus isikuandmete kaitse õiguse tagamisel infoühiskonnas ja nende võimalikest arengutest, magistritöö, Tartu Ülikooli Õigusteaduskond 2015, lk 29.

<sup>9</sup> § 19, p 3.1.2.1. Põhiõigused ja Vabadused. II peatükk. Eesti Vabariigi põhiseadus. Kommenteeritud väljaanne. [www.pohiseadus.ee/ptk-2/](http://www.pohiseadus.ee/ptk-2/) (09.12.2016).

<sup>10</sup> *Ibid.*

<sup>11</sup> Tikk, E., Nõmper, A. Informatsioon ja õigus. Tallinn, Juura 2007, lk 47.

<sup>12</sup> RKHKo 3-3-1-3-12, p 19.

<sup>13</sup> EKo 09.11.2010, C-92/09 ja C-93/09, *Volker und Markus Schecke, Hartmut Eifert*, p 47.; EKo 24.11.2011, C-468/10 ja C-469/10, *ASNEF ja FECEMD*, p 41.

<sup>14</sup> IKS RT I, 06.01.2016, 10.

<sup>15</sup> *Ibid.*, § 1, lg 1.

<sup>16</sup> Pilving, I. Õigus isikuandmete kaitsele. *Juridica VIII*, 2005, lk 533.

<sup>17</sup> RKTKo 3-2-1-159-14, p 13; Tammer, S. Kujutis kui tegelikult kaitstav õigushüve. *Juridica IX/2011*, lk 653.

võimalik konkreetse isikuga seostada ning isikuandmeteks on ka heli- ja pildiandmed<sup>18</sup>. Muuhulgas sõnastab IKS § 5 isikuandmete töötlemise, mis on iga isikuandmete toiming, sealhulgas isikuandmete kogumine, salvestamine, korrastamine, säilitamine, muutmine ja avalikustamine, juurdepääsu võimaldamine isikuandmetele, päringute teostamine ja väljavõtete tegemine, isikuandmete kasutamine, edastamine, riskasutamine, ühendamise, sulgemine, kustutamine või hävitamine, või mitu eelnimetatud toimingut, sõltumata toimingute teostamise viisist ja kasutatavatest vahenditest. IKS ei kohaldu, kui isikuandmeid töötleb füüsiline isik isiklikul otstarbel<sup>19</sup>. Suure tõenäosusega kaotab senisel kujul IKS Euroopa Parlamendi ja nõukogu määruse 679/2016 rakendamisel kehtivuse, kuivõrd see tugineb direktiivile 95/46/EÜ, mille määrus 679/2016 tunnistab kehtetuks<sup>20</sup>.

Isikuandmed on seega Eesti seadusandlusega kaitstud, kuid on väga laialt tõlgendatavad. Üha rohkem väljakutseid esitab Eestis ja ka mujal maailmas isikuandmete kaitsele Internet, kus jagatakse palju informatsiooni ja sageli ka näiteks teadmatuses rikutakse seadust.

*Expressis verbis* kaamerate kasutamist ei ole veel Eestis tänaseni ühegi seadusega reguleeritud, kuid AKI on koostanud juhendi “Juhend kaamerate kasutamise kohta”<sup>21</sup>, mis ei ole küll kuidagi õiguslikult siduv, vaid pigem soovituslik ja selgitav. Juhend on koostatud eesmärgiga anda juhiseid IKS-i paremaks rakendamiseks ning aitab paremini mõista, kuidas kasutada kaameraid nii, et see tegevus oleks kooskõlas IKS sätetega<sup>22</sup>. Seega puudub riigisisises isikuandmete kaitse õiguses õiguslikult siduv spetsiifiline kaameraid puudutav regulatsioon ning lähtuda tuleb IKSist kui üldregulatsioonist ning abistavatest juhenditest nagu AKI juhend kaamerate kasutamise kohta.

---

<sup>18</sup> Tammer, *supra* nota 17, lk 653.

<sup>19</sup> IKS, *supra* nota 14, § 2, lg 1, p 1.

<sup>20</sup> Euroopa Parlamendi ja nõukogu 27. aprilli 2016 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).

<sup>21</sup> Andmekaitse Inspeksioon. Juhend kaamerate kasutamise kohta, 2016. [www.aki.ee/sites/www.aki.ee/files/elfinder/article\\_files/kaamerate%20juhis%20\(01.07.2016\).pdf](http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/kaamerate%20juhis%20(01.07.2016).pdf) (21.11.2016)

<sup>22</sup> *Ibid*, lk 3.

## 1.2 Isikuandmete kaitse õiguslik raamistik Euroopas

Üldised reeglid isikuandmete kaitse tagamiseks Euroopa Liidus sätestab 1995. aasta Euroopa Ühenduse direktiiv 95/46/EÜ (edaspidi andmekaitse direktiiv)<sup>23</sup>, mis on Euroopa Liidu andmekaitse alus<sup>24</sup>. Aastal 2000 hakkas kehtima Euroopa Liidu põhiõiguste harta (edaspidi harta), mis andis isikuandmete kaitsele põhiõiguse staatuse<sup>25</sup>, kuid jäi esialgu üksnes õiguste deklaratsiooniks<sup>26</sup>. Kui esialgu oli harta kõigest poliitiline dokument, siis 2009. aastal koos Lissaboni lepinguga muudeti harta liikmesriikidele õiguslikult siduvaks<sup>27</sup>. 2016. aasta 4. mail avaldati Euroopa Liidu Teatajas isikuandmete kaitse üldmäärus<sup>28</sup> (edaspidi üldmäärus). Üldmäärusega tunnistatakse kehtetuks andmekaitse direktiiv ning see on tervikuna siduv ning vahetult kohaldatav kõikides liikmesriikides<sup>29</sup>. Üldmäärus jõustus 2016. aastal ning kohaldatakse alates 25. maist 2018. aastal<sup>30</sup>.

Andmekaitse direktiiv sündis, kuna juba kehtinud Euroopa Nõukogu konventsioon isiku kaitseks isikuandmete töötlemisel ning Majanduskoostöö ja Arengu Organisatsiooni (OECD) soovitusel isikuandmete ja privaatsuse kaitseks olid soovituslikud, mis jätsid riikidele vabad käed ja tagajärjeks oli aktide ebaühtlane rakendamine<sup>31</sup>. Näiteks Saksamaal, Prantsusmaal ja Suurbritannias olid tekkinud isikuandmete ja privaatsuse kaitsele tugevad traditsioonid, mis Kreekal puudusid<sup>32</sup>. Andmekaitse direktiivi artikkel 1 sätestab, et liikmesriigid kaitsevad isikuandmete töötlemisel füüsiliste isikute põhiõigusi ja -vabadusi ning eelkõige nende õigust eraelu puutumatusele<sup>33</sup>. Ühtlasi defineerib artikkel 2 isikuandmed kui igasuguse teabe tuvastatud või tuvastatava füüsilise isiku kohta ning tuvastatav isik on isik, keda saab otseselt või kaudselt tuvastada, eelkõige isikukoodi põhjal või ühe või mitme tema füüsilisele, füsioloogilisele,

<sup>23</sup> Kungas, *supra* nota 8, lk 25; Kuner, C. The European Union and the Search for an International Data Protection Framework. Groningen Journal of International Law, vol. 2, ed. 1: Privacy in International Law, lk 58.

<sup>24</sup> Gundermann, L. Euroopa Liidu andmekaitse õigus – andmekaitse ja andmetele avaliku juurdepääsu suhtest ning andmekaitse järelevalve olukorrast. Juridica VIII/2005, lk 511.

<sup>25</sup> Kungas, *supra* nota 8, lk 22.

<sup>26</sup> Euroopa Parlament. Euroopa Liidu põhiõiguste harta, 2016. [www.europarl.europa.eu/atyourservice/et/displayFtu.html?ftuId=FTU\\_1.1.6.html](http://www.europarl.europa.eu/atyourservice/et/displayFtu.html?ftuId=FTU_1.1.6.html) (03.04.2017).

<sup>27</sup> Kungas, *supra* nota 8, lk 23

<sup>28</sup> Euroopa Liidu Teataja, L 119, 4. mai 2016

<sup>29</sup> OJ L 119, 04.05.2016.

<sup>30</sup> *Ibid.*

<sup>31</sup> Ilus, T. Isikuandmete kaitse olemus ja arengusuunad. Juridica VII/2002, lk 437; De Hert, P., Papakonstantinou, V. The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals. Computer law & security review 28 (2012), lk 132.

<sup>32</sup> Rustad, M.L., Kulevska, S, Reconceptualizing the Right To Be Forgotten To Enable Transatlantic Data Flow. Harvard Journal of Law & Technology, 2015, vol 28, lk 359.

<sup>33</sup> OJ L 281, 23.11.1995.

vaimsele, majanduslikule, kultuurilisele või sotsiaalsele identsusele omase joone põhjal<sup>34</sup>. See tunnuste loetelu aga ei ole ammendav, vaid näitlik, kuidas isikut tuvastada võib ning teabe sisu ei ole tähtis – piisab, et teave on isiklik ja selle kaudu on võimalik isik tuvastada<sup>35</sup>. Andmekaitse direktiiv on väga oluline, kuna see on sisustanud isikuandmete mõiste kui õigusmõiste, määratlenud isikute õigused ja sätestanud nõuded delikaatsete isikuandmete töötlemisega seoses<sup>36</sup>. Artikkel 22 annab kõikidele isikutele õiguse kasutada õiguskaitsevahendeid, kui nende õigusi on rikutud ning artikkel 23 annab õiguse ebaseadusliku andmete töötlemise tagajärjel tekkinud kahju kompensatsiooniks<sup>37</sup>.

Hartat oli vaja, et välja töötada ühistel põhiväärtustel rajanev Euroopa visioon<sup>38</sup>. See on ainus maailma tasemel õigusakt, milles on õigus isikuandmete kaitsele sätestatud iseseisva põhiõigusena<sup>39</sup>. Euroopa Liidu põhiõiguste harta artikkel 7 sätestab, et igal inimesel on õigus sellele, et austataks tema era- ja perekonnaelu, kodu ja edastavate sõnumite saladust<sup>40</sup>. Sama harta artikkel 8 on pühendatud isikuandmete kaitsele ning sätestab, et igal inimesel on õigus isikuandmete kaitsele, neid tuleb töödelda kindlatel eesmärkidel, kas isiku nõusolekul või seaduses ettenähtud õiguslikul alusel<sup>41</sup>. Lisaks on artikkel 8 järgi õigus igal inimesel tema kohta kogutud andmetega tutvuda ning nõuda nende parandamist<sup>42</sup>.

Kuigi kehtiv raamistik on Euroopa Komisjoni arvates endiselt asjakohane oma eesmärkide ja põhimõtete seisukohalt, on ta siiski veidi jalgu jäänud tehnoloogia kiirele arengule<sup>43</sup>. Näitena võib siia tuua pilveteenuste arengu. Olukorda peaks parandama üldmäärus, mille suhtes rahvusvahelises õiguskirjanduses jäädakse aga eriarvamusele<sup>44</sup>. Näiteks laiendatakse

---

<sup>34</sup> *Ibid.*

<sup>35</sup> Pilving, I. Sugupuud müügiks ja roolijoodikud häbiposti? Isikuandmetega seonduvad piirangud avaliku teabe avaldamisel. *Juridica* II/2004, lk 77.

<sup>36</sup> Kungas, *supra* nota 8, lk 28.

<sup>37</sup> OJ L 281, 23.11.1995; *Ibid.*, lk 26.

<sup>38</sup> Tupay, P. T. Õigusest eraelule kuni andmekaitse üldmääruseni ehk tundmatu õigus isikuandmete kaitsele. *Juridica* IV/2016, lk 231.

<sup>39</sup> *Ibid.*

<sup>40</sup> OJ C 83, 30.3.2010.

<sup>41</sup> *Ibid.*

<sup>42</sup> *Ibid.*

<sup>43</sup> Kungas, *supra* nota 8, lk 28; Komisjoni teatis euroopa parlamendile, nõukogule, majandus- ja sotsiaalkomiteele ning regioonide komiteele. Terviklik lähenemisviis isikuandmete kaitsele Euroopa Liidus, 2010. [ec.europa.eu/justice/news/consulting\\_public/0006/com\\_2010\\_609\\_et.pdf](http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_et.pdf) (04.03.2017). ja Robinson, N., Graux, H., Botterman, M., Valeri, L. Review of the European Data Protection Directive. Cambridge, Rand Europe 2009, lk 18.

<sup>44</sup> Kotschy, W. The proposal for a new General Data Protection Regulation—problems solved? *International Data Privacy Law*, 2014, Vol. 4, No. 4, lk 275; Buitelaor, J.C. Pprivacy: Back to the Roots. *German Law Journal* 13 *German L.J.* (2012), lk 171.

üldmäärusega isikuandmete mõistet, kuhu on lisandunud asukohateave ja võrguidentifikaator<sup>45</sup>. Ehk siis isikuandmeteks võivad olla ka näiteks IP-aadress ja “küpsised” (i.k. *cookies*) või muud andmed, mida võidakse kasutada füüsiliste isikute profileerimiseks ja nende tuvastamiseks<sup>46</sup>. Üldmääruse kaks peamist eesmärki on suurendada isikute kontrolli oma isikuandmete üle ning pakkuda juriidilistele isikutele juriidilist kindlustunnet ning vähendada administratiivset koormust<sup>47</sup>. Üldmäärust ei kohaldata, kui isikuandmeid töödeldakse muu kui liidu õiguse kohaldamisalasse kuuluva tegevuse käigus, isikuandmeid töödeldakse ühise välis- ja julgeolekupoliitika kohaldamisalasse jääva tegevuse käigus, isikuandmeid töötleb füüsiline isik eranditult isiklike või koduste tegevuste käigus ning kui isikuandmeid töötlevad pädevad asutused süütegudega seoses<sup>48</sup>.

Ka Euroopa õigusaktidega ei ole sarnaselt Eestile otseselt kaamerate kasutamine reguleeritud ning seda ei tee ka kehtima hakkav üldmäärus<sup>49</sup>. Seega tuleb lähtuda veel bakalaureusetöö kirjutamise hetkel kehtivas andmekaitseinspektsiooni sättestatust ning alates 25. maist 2018 üldmääruses sättestatust.

### 1.3 Salvestamine isiklikuks otstarbeks

Seoses nutitelefonide ja auto pardakaamerate üha populaarsemaks<sup>50</sup> muutumisega on saanud võimalikuks laiaulatuslik ümbritseva info salvestamine, mis muu hulgas võib hõlmata ka isikuandmeid. Seda infot on võimalik hiljem Internetti kõigile vaatamiseks üles laadida, samas jätta ka ainult endale kasutamiseks ja vaatamiseks. Viimasel juhul on tegemist isikuandmete töötlemisega isiklikuks otstarbeks. Kui füüsiline isik töötleb isikuandmeid isiklikul otstarbel, siis IKS ei kohaldu<sup>51</sup>. Isiklik otstarve tähendab, et isik võib filmida ja pildistada ükskõik kus ja ükskõik mida ilma kellelki luba küsimata seni, kuni ta seda kuskil ei avalda<sup>52</sup>. Ka 2018. aastal kehtima

---

<sup>45</sup> OJ L 119, 04.05.2016, art 4.

<sup>46</sup> *Ibid*, p 30.

<sup>47</sup> Rustad, Kulevska, *supra* nota 32, lk 367.

<sup>48</sup> OJ L 119, 04.05.2016, art 2, lg 2.

<sup>49</sup> Štītilis, D., Laurinaitis, M. Legal regulation of the use of dashboard cameras: Aspects of privacy protection. *Computer law & security review* 32 (2016), lk 319.

<sup>50</sup> Credence Research, 3 nota 3.

<sup>51</sup> IKS, *supra* nota 14, § 2, lg 1, p 1.

<sup>52</sup> Andmekaitse Inspektsioon (2016), *supra* nota 21, lk 5.

hakkava üldmääruse artikkel 2 sätestab, et määrust ei kohaldata, kui isikuandmeid töötleb füüsiline isik eranditult isiklike või koduste tegevuste käigus<sup>53</sup>.

Isiklik otstarve tähendab, et füüsiline isik võib salvestisi jagada oma perega või sõpradega, kes ise ka konkreetsel salvestisel on<sup>54</sup>. Ehk siis salvestis peab jääma sellesse kitsasse ringkonda, keda salvestisel kajastatud on ning sotsiaalmeediasse või videokeskcondadesse materjali üleslaadimine ilma salvestusel olevate isikute nõusolekuta ei ole lubatud. Väga populaarsed on tänapäeval ka erinevad pilveteenused, kus sinna laetud failid ei ole füüsiliselt isiku käes. Võib tekkida küsimus, kas see kvalifitseerub isikliku otstarbe või avalikult jagamise alla. Kui pilveteenusesse laetud failid on turvatud parooliga ning neile on ligipääs ainult failide töötlejal või salvestistel olevatel inimestel, siis siin vastuolusid ei teki ning tegemist on isiklikuks otstarbeks töötlemisega<sup>55</sup>. Pilveteenusega kaasnevad aga erinevad turvariskid, sest pilveteenus on täpselt nii turvaline kui turvalised on seadmed, mis on sinna ühendatud. Rahvusvahelises õiguskirjanduses on välja toodud, et pilveteenusega ühendatud nutitelefon võib olla sama võimas tööriist kui sinna ühendatud arvuti<sup>56</sup>. Võib eeldada, et isiklikuks otstarbeks salvestamise kategooriasse kuulub ka salvestamine oma vara kaitseks üles pandud statsionaarsete turvakaameratega, kuid alati ei töötle isik isikuandmeid sellisel juhul isiklikul otstarbel. Isiklikul otstarbel töötleb isik andmeid vaid siis, kui tema turvakaamera vaatevälja jääb ainult tema valduses olev maa-ala ning siis ka IKS-i ei kohaldata<sup>57</sup>. Siit võib järeldada, et kui kaamera vaatevälja jääb ka avalik ruum, ei ole enam tegemist isiklikuks otstarbeks salvestamisega. Samale järeldusele on jõudnud ka Euroopa Kohus *Ryneš*'i kaasuses.<sup>58</sup> Kui tegemist ei ole isiklikuks otstarbeks salvestamisega, tuleb andmetöötlejal täita IKS § 14 lg-s 3 sätestatud kolm tingimust, mis peavad olema täidetud korraga: ei tohi kahjustada ülemääraselt andmesubjekti õigustatud huve, andmeid kasutatakse eesmärgipäraselt ja jälgimisseadmete kasutamisest tuleb teavitada. Nõue ei laiene jälgimisseadmetiku kasutamisele riigiasutuse poolt seaduses sätestatud alustel ja korras<sup>59</sup>.

Ülalolevat silmas pidades võib tekkida õigustatud küsimus, kas auto pardakaameraga salvestamine kvalifitseerub ikkagi isikuandmete isiklikuks otstarbeks töötlemise alla, kuna auto pardakaamera

<sup>53</sup> OJ L 119, 04.05.2016, art 2, lg 2, p c.

<sup>54</sup> Andmekaitse Inspektsioon (2016), *supra* nota 21, lk 6.

<sup>55</sup> *Ibid.*

<sup>56</sup> De Filippi, P., Belli, L. Law of the Cloud v Law of the Land: Challenges and Opportunities for Innovation. European Journal of Law and Technology, Vol 3, Issue 2, 2012, lk 2.

<sup>57</sup> Andmekaitse Inspektsioon (2016), *supra* nota 21, lk 13.

<sup>58</sup> EKo 11.12.2014, C-212/13, *Ryneš*, p 35.

<sup>59</sup> IKS, *supra* nota 14, § 14, lg 3.

filmib ka avalikku ruumi. *Ryneš'*i kaasus auto pardakaameraid ei puuduta. AKI on meedia vahendusel avaldanud üksnes seisukoha, et seni, kuni ei ole pardakaamera videol äratuntavaid inimesi, on videote avalik jagamine lubatud<sup>60</sup>. Ühtlasi võivad salvestisel olla katmata autode registreerimisnumbrid, kuna vastav register ei ole avalik ning auto registreerimisnumbri järgi ei ole võimalik isikut tuvastada<sup>61</sup>. Eeltoodust tulenevalt allub auto pardakaamera salvestis pigem muu salvestava tehnoloogia reeglitele kui statsionaarse turvakaamera piirangutele.

Kokkuvõtvalt on andmetöötaja vastutus välistatud ja tegemist isiklikuks otstarbeks salvestamisega tegemist, kui salvestis jääb töötaja või salvestisel oleva kitsa isikute ringi käsutusse. Kui salvestise säilitamiseks kasutatakse pilveteenust, siis peab olema salvestis turvatud selliselt, et sellele pääseks ligi kas ainult töötaja või salvestisel olevad isikud. Statsionaarse turvakaamera puhul on tegemist isiklikuks otstarbeks salvestamisega ainult juhul, kui salvestisel on kajastatud ainult töötaja valduses olev maa-ala, mitte avalik ruum.

#### 1.4 Salvestise avaldamine

Mida rohkem isikud erinevate seadmetega infot salvestavad ja mida rohkem on võimalusi enda salvestiste avaldamiseks, seda enam võib ette tulla füüsiliste isikute privaatsuse või õiguste rikkumisi. Rahvusvahelises õiguskirjanduses<sup>62</sup> on välja toodud kolm peamist arengusuunda, mis meie privaatsust mõjutavad: üha rohkem toodetakse andmeid, millega kaasneb üha suurema hulga isikuandmete kogumine, andmed globaliseeruvad ning üha keerulisem on seda kõike kontrollida. Igapäevaselt inimesed ei pruugigi alati sellele mõelda, et kui nad lisavad sotsiaalmeediasse mingi video või pildi, siis nad võivad sellega rikkuda teiste isikute õigusi. Tõenäoliselt ei juhtu midagi, kui isik sõpradega ühisel koosviibimisel tehtud foto näiteks oma *Facebooki* sotsiaalmeediakonto seinale laeb. Teisiti võib aga minna siis, kui isiku kaamera või fotoaparaadi ette jääb midagi, mis paneb selle materjali Internetis kiiresti levima ning see kontrolli alt väljub. Sellistel puhkudel ei soovi ilmselt sellele materjalile jäänud inimesed enam sellel materjalil olla ning soovivad selle eemaldamist. Salvestise eemaldamisest võib aga olla sellisel juhul juba vähe abi, sest salvestis on

---

<sup>60</sup> Postimees: AKI hajutab lugejate kahtlusi, 2015. [www.aki.ee/et/uudised/meediakajastus/postimees-aki-hajutab-lugejate-kahtlusi](http://www.aki.ee/et/uudised/meediakajastus/postimees-aki-hajutab-lugejate-kahtlusi) (14.01.2017).

<sup>61</sup> *Ibid.*

<sup>62</sup> DeVries, W.T., Protecting Privacy in the Digital Age, Berkeley Technology Law Journal 18 Berkeley Tech. L.J. (2003), lk 291.

n-ö “hakanud elama oma elu”. Millistel juhtudel siis ikkagi võib töötleja oma salvestise avaldada ja millistel juhtudel ta seda kindlasti teha ei tohiks?

#### 1.4.1 Juhud, kus isikuandmete avaldamine on lubatud

##### 1.4.1.1 Andmesubjekti nõusolek

IKS sätestab § 10 lg-s 1, et isikuandmete töötlemine on lubatud üksnes andmesubjekti nõusolekul, kui seadus ei sätesta teisiti:

- andmesubjekti nõusolek on kehtiv ainult siis, kui see on tema vaba tahe;
- nõusolekus peavad olema selgelt määratletud andmed, mille töötlemiseks luba antakse, andmete töötlemise eesmärk ning isikud, kellele andmete edastamine on lubatud;
- nõusolek peab sisaldama andmete kolmandatele isikutele edastamise tingimused ning andmesubjekti õigused tema isikuandmete edasise töötlemise osas;
- vaikimist või tegevusetust nõusolekuks ei loeta;
- nõusolek võib olla osaline ja tingimuslik.

IKS § 12 lg-tes 2-8 on sätestatud ka muud nõusolekule kehtivad tingimused:

- vorm peab olema kirjalikku taasesitamist võimaldavas vormis, kuid IKS jätab võimaluse ka muudeks vormideks, kui vorminõude järgmine ei ole andmetöötlemise erilise viisi tõttu võimalik;
- töötleja on kohustatud enne nõusoleku küsimist tegema teatavaks enda nime, aadressi ja kontaktandmed;
- delikaatsete isikuandmete töötlemisel tuleb isikule selgitada, et tegemist on delikaatsete isikuandmetega ning võtta nõusolek;
- nõusolek kehtib andmesubjekti eluajal ning 30 aastat pärast tema surma, kui andmesubjekt ei ole otsustanud teisiti;
- nõusoleku võib andmesubjekt igal ajal tagasi võtta, kuid sellel ei ole tagasiulatuvat jõudu;
- vaidluste korral kehtib eeldus, et nõusolekut ei ole antud;
- nõusoleku tõendamise kohustus lasub isikuandmete töötlejal<sup>63</sup>.

---

<sup>63</sup> Vt ka Andmekaitse Inspektsioon (2016), *supra* nota 21, lk 19-20.

Isikuandmete kaitse üldmääruses on andmesubjekti nõusolek defineeritud kui vabatahtlik, konkreetne, teadlik ja ühemõtteline tahteavaldus, millega andmesubjekt kas avalduse vormis või selge nõusolekut väljendava tegevusega nõustub tema kohta käivate isikuandmete töötlemisega<sup>64</sup>.

Nõusolekuks ei saa pidada vaikimist, eelnevalt märgistatud lahtreid või tegevusetust<sup>65</sup>. See tähendab, et näiteks, kui on andmetöötleja valmistanud ette spetsiaalse veebilehe, kus andmesubjekt saab oma nõusoleku anda, siis ei tohiks ükski lahter olla eelnevalt täidetud. Ühtlasi ei saa pidada nõusolekuks, kui näiteks andmetöötleja saadab andmesubjektile e-postiga kirja, kus on klausel, et antud kirjale vastamata jätmisel on nõusolek vaikimisi antud. Näiteks auto pardakaameraga salvestamisel ei saa pidada nõusolekuks pelgalt fakti, et isik on salvestisel, ei vältinud kuidagi salvestisele jäämist ning seega oli salvestamisega nõus<sup>66</sup>.

AKI on seisukohal, et näiteks videomaterjali salvestamisel on võimalik tõendada nõusoleku olemasolu ka filmimise teel, kus lihtsalt andmesubjekti nõusolek tuleks filmida üles enne materjali enda filmimist<sup>67</sup>. Auto pardakaamerate puhul ei tuleks ilmselt selline olukord kõne alla juba seetõttu, et kaamera asub autos sees ja andmesubjekt väljas ning kaamerani ei jõuaks heli. Kui aga nii andmetöötleja kui ka andmesubjekt väga soovivad ja piisavalt vaeva näevad, siis tehniliselt oleks sellisel viisil võimalik nõusolek võtta. Kui sellises olukorras tekib vaidlus nõusoleku olemasolu või puudumise kohta, tuleb hinnata, millist tahet andmesubjekti käitumine peegeldab<sup>68</sup>. Sellisel juhul tuleb tõlgendada andmesubjekti miimikat, vastuseid, kogu situatsiooni ja ümbritsevat olustikku tsiviilseadustiku üldosa seaduse § 68 lg 3 tähenduses<sup>69</sup>. Selle tulemusena peaks tekkima veendumus, kas andmesubjekt nõustus enda jäädvustamise ning salvestise avaldamisega või mitte<sup>70</sup>. Autori hinnangul aga ei ühti sellisel kujul nõusolek üldmääruse põhimõttega, et nõusolek peab olema konkreetne ja ühemõtteline tahteavaldus<sup>71</sup>.

Nõusolek peab vastama väga paljudele tingimustele ning on vähetõenäoline, et lihtsa foto või video üleslaadimiseks füüsilisest isikust töötlejad kõike korrektselt vormistama hakkavad. Paljudel juhtudel ei ole see enam isegi tagantjärele võimalik, sest spontaanselt tänaval tehtud heale

---

<sup>64</sup> OJ L 119, 04.05.2016, art 4, p 11.

<sup>65</sup> OJ L 119, 04.05.2016, pp 32.

<sup>66</sup> Tammer, *supra* nota 17, lk 655.

<sup>67</sup> Andmekaitse Inspeksioon (2016), *supra* nota 21, lk 19.

<sup>68</sup> Tammer, *supra* nota 17, lk 654.

<sup>69</sup> *Ibid*; TsÜS RT I, 12.03.2015, 106.

<sup>70</sup> Tammer, *supra* nota 17, lk 654.

<sup>71</sup> OJ L 119, 04.05.2016, art 4, p 11.

pildile või videole jäänud inimestega kontakti saamine on keeruline. Sellisel juhul on võimalik andmesubjekt muuta salvestisel tundmatuks.

Riigikohus on leidnud, et IKS kaitseb andmesubjekti ka korduva avaldamise eest isegi, kui isik on mingis vormis avaldamisele nõusoleku andnud<sup>72</sup>. Andmete esialgne ja korduv avalikustamine võivad toimuda väga erinevas vormis ja väga erineva intensiivsusega, sõltuvalt andmete edastaja isikust, infokanalist, kontekstist, auditooriumist jne<sup>73</sup>. Seega kui näiteks andmesubjekt on andnud töötlejale nõusoleku pardakaamera video avaldada enda blogis, mille lugejaskond on näiteks 100 inimest, siis see ei anna veel volitust videot avaldada meedias. Seega, kui töötlemisel on mitu eesmärki, tuleb andmesubjektilt nõusolek saada kõigi nende eesmärkide kohta<sup>74</sup>.

Eelnevast tulenevalt võib järeldada, et andmetöötaja vastutuse välistamiseks on vajalik salvestise avaldamise korral andmesubjekti nõusolek, mis peab põhinema tema vabal tahtel, olema konkreetne, teadlik ja ühemõtteline ning ei tohi olla tagasi võetud. Muuhulgas peab andmetöötaja arvestama, et nõusoleku olemasolu tõendamiskohustus lasub temal.

#### 1.4.1.2 Ajakirjanduslik eesmärk ja avalik huvi

IKS jätab võimaluse andmesubjekti nõusolekuta andmeid töödelda ajakirjanduslikul eesmärgil, kui selleks on ülekaalukas avalik huvi, see on kooskõlas ajakirjanduseetika põhimõtetega ning see ei kahjusta ülemäära andmesubjekti õigusi<sup>75</sup>. Tähtis on, et kõik need tingimused peavad esinema korraga<sup>76</sup>.

Õiguskirjanduses ollakse arvamusel, et terminit “ajakirjanduslik eesmärk” ei saa käsitleda kitsalt, vaid ajakirjanduslik eesmärk peaks olema juba see, kui üks isik avaldab infot tundmatule kolmandale isikule<sup>77</sup>. See tagab selle, et IKS kohalduks kõikidele avalikustajatele ühiselt<sup>78</sup>. Seega saab ajakirjanduslikul eesmärgil avaldamiseks pidada näiteks füüsilisest isikust andmetöötaja poolt avaldatud pardakaamera video sotsiaalmeedias.

---

<sup>72</sup> RKHKo 3-3-1-3-12, p 24; Kungas, *supra* nota 8, lk 32.

<sup>73</sup> RKHKo 3-3-1-3-12, p 24.

<sup>74</sup> OJ L 119, 04.05.2016, pp 32.

<sup>75</sup> IKS, *supra* nota 14, § 11, lg 2; RKTKo 3-2-1-159-14, p 14.

<sup>76</sup> Andmekaitse Inspeksioon (2016), *supra* nota 21, lk 15; RKTKo 3-2-1-159-14, p 14.

<sup>77</sup> Tammer, *supra* nota 17, lk 657.

<sup>78</sup> *Ibid.*

Ülekaalukas avalik huvi tähendab, et ajakirjandus ei või nõusolekuta kajastada isikut või selle isikuga seotud sündmust, kui tema vastu puudub avalik huvi<sup>79</sup>. Avalik huvi kuulub määratlemata õigusmõistete hulka, mis on ajas muutuvad ja väga laiade tunnustega ning nende ammendav defineerimine on võimatu<sup>80</sup>. Avalik huvi mõtestatakse lahti konkreetse kaasuse kontekstis ning igaks juhtumiks sobiva definitsiooni andmine on võimatu<sup>81</sup>. Õiguskirjanduses on välja toodud, et avalik huvi on olemas, kui see tekitab elava debati ja asja vastu tunneb huvi suurem hulk inimesi, kui vastava sündmusega seotud isikute ring on<sup>82</sup>. Ühtlasi peab avalik huvi olema tegelik, põhjendatud ning seda ei tohi segi ajada uudishimu ja kommertshuviga<sup>83</sup>.

Avaliku elu tegelane on isik, kes on pidanud arvestama, et tema vastu on kõrgendatud avalikkuse tähelepanu, kuid seejuures ei tohi ka tema õigusi ülemääraselt rikkuda<sup>84</sup>. Ühtlasi on avaliku elu tegelane isik, kes teenib elatist enda isiku või loomingu eksponeerimisega<sup>85</sup>. Riigikohus on seisukohal, et avaliku elu tegelane on isik, kes teostab avalikku võimu või suudab mõjutada poliitikat või majandust<sup>86</sup>.

Ajakirjandus peab alati eraldi hindama kas avalik huvi üldsust huvitavate avaliku elu tegelaste andmete avalikustamiseks on niivõrd oluline, et kaalub üles avaliku elu tegelase ja teiste isikute õiguste kaitse vajaduse<sup>87</sup>. Alati ei pruugigi olla avaldajaks ajakirjandus, vaid oluline on pigem, kas avaldatul on ajakirjanduslik eesmärk<sup>88</sup>. Euroopa Inimõiguste Kohtu seisukoht on, et ajakirjanduslik eesmärk on informatsiooni või ideede levitamine, mis aitab edendada debatti avaliku huvi orbiidis olevatel teemadel<sup>89</sup>.

---

<sup>79</sup> Isikuandmete kaitse seaduse eelnõu seletuskiri. [www.aki.ee/sites/www.aki.ee/files/elfinder/article\\_files/IKS%20SELETUSKIRI%20%281%29.rtf](http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/IKS%20SELETUSKIRI%20%281%29.rtf) (14.01.2017), § 11.

<sup>80</sup> Ikkonen, K. Avalik huvi kui määratlemata õigusmõiste. *Juridica* III/2005, lk 187.

<sup>81</sup> *Ibid.*, lk 198.

<sup>82</sup> Tammer, *supra* nota 17, lk 657.

<sup>83</sup> Aleksejeva, P. Isikust tehtud kujutise avaldamise õiguspärasus, magistritöö, Tartu Ülikooli Õigusteaduskond 2013, lk 52.

<sup>84</sup> Isikuandmete kaitse seaduse eelnõu seletuskiri, *supra* nota 79, § 11.

<sup>85</sup> Eesti Ajalehtede Liit. Eesti ajakirjanduseetika koodeks, 1998. [www.eall.ee/eetikakoodeks.html](http://www.eall.ee/eetikakoodeks.html) (14.01.2017), p 1.6.

<sup>86</sup> RKHKo 3-3-1-85-15, p 4.

<sup>87</sup> Isikuandmete kaitse seaduse eelnõu seletuskiri, *supra* nota 79, § 11.

<sup>88</sup> Andmekaitse Inspeksioon (2016), *supra* nota 21, lk 15.

<sup>89</sup> *Ibid.*; EIKo 26.11.1991, 13585/88, *Observer and Guardian v. The United Kingdom*, p 5.2.

Meediakajastus peab olema kooskõlas heade kommete ja ajakirjanduseetika põhimõtetega, mis tulenevad Eesti Ajalehtede Liidu poolt koostatud Eesti ajakirjanduseetika koodeksist<sup>90</sup>. Näiteks ei tohi ajakirjandus kellelgi tekitada põhjendamatuid kannatusi veendumata, kas avalikkusel tõesti on vaja vastavat informatsiooni teada<sup>91</sup>. Nõusolekuta võib avaldada infot, mis on seotud avaliku elu tegelase avaliku ülesandega, ainult eraelu kajastava info avaldamine üldsuse uudishimu rahuldamiseks ja kasu saamiseks ei ole lubatud<sup>92</sup>.

Septembris 2016. aastal ringles sotsiaalmeedias ja veebiväljaannetes auto pardakaamera salvestis, kus Juhan Parts unustas peale tankimist auto paaki tankuri püstoli ning sõitis ära<sup>93</sup>. Selle tulemusel katkes voolik ja püstol jäi Juhan Partsi auto paaki, mille tanklatöötaja sealt eemaldas. Juhan Parts on tuntud poliitik ja ilmselt ei saa tekkida kahtlust, kas ta on avaliku elu tegelane. Küsimus on hoopis selles, kas antud õnnetus tanklas on avalikes huvides ja aitab edendada avalikku debatti. Videos ei saanud keegi kannatada ja võimalikud kriimud Juhan Partsi autol või tanklale tekitatu kahju korvas kindlustus. Nagu antud peatüki sissejuhatavas lõigus juba mainitud, siis salvestise andmesubjekti loata avaldamine on lubatud, kui esineb ülekaalukas avalik huvi, see on kooskõlas ajakirjanduseetika põhimõtetega ning see ei kahjusta ülemäära andmesubjekti õigusi<sup>94</sup>.

Autori hinnangul puudub antud juhtumi vastu ülekaalukas avalik huvi, kuna inimesed kannatada ei saanud ning kannatada saanud vara ei kuulu avalikule võimule. Juhan Partsi videos olev auto kajastub küll ka Juhan Partsi kuluhüvitistes<sup>95</sup>, kuid see ei tee sellest autost riigile kuuluvat vara, mille kahjustada saamisel oleks avalik huvi kindlasti olemas. Video avaldamine on autori hinnangul kooskõlas ajakirjanduseetika põhimõtetega ning ei kahjusta ka Juhan Partsi õigusi. Kuna aga kõik IKS-is toodud kolm tingimust peavad esinema korraga<sup>96</sup>, siis oleks autori hinnangul pidanud ülekaaluka avaliku huvi puudumisel antud video avaldamata jätma.

---

<sup>90</sup> Isikuandmete kaitse seaduse eelnõu seletuskiri, *supra* nota 79, § 11.

<sup>91</sup> Eesti Ajalehtede Liit, *supra* nota 85, p 1.5.

<sup>92</sup> Aleksejeva, *supra* nota 83, lk 39.

<sup>93</sup> Postimees. Video: Juhan Parts lõhkus bensiinijaamas tankuri. [tallinncity.postimees.ee/3853807/video-juhan-parts-lohkus-bensiinijaamas-tankuri](http://tallinncity.postimees.ee/3853807/video-juhan-parts-lohkus-bensiinijaamas-tankuri) (28.01.2017)

<sup>94</sup> IKS, *supra* nota 14, § 11, lg 2.

<sup>95</sup> Eesti Maksumaksjate Liit. Riigikogu liikmetele makstud kuluhüvitised sõiduautode rendi ja liisingu eest, 2015. [www.maksumaksjad.ee/modules/news/article.php?storyid=8354](http://www.maksumaksjad.ee/modules/news/article.php?storyid=8354) (28.01.2017).

<sup>96</sup> Andmekaitse Inspeksioon (2016), *supra* nota 21, lk 15.

Teine näide pärineb 2016. aasta maikuust, kui sotsiaalmeedias levis pardakaamera salvestis<sup>97</sup> mehest, kes teostab äkilise keelatud manöövri ja taga sõitva auto juht talle pahameelest tingituna signaali annab. Eesmise auto juht otsustab peatuda, ei lase tagumise auto juhil sõitu jätkata ning väljub oma autost pesapallikurikaga ning käitub tagumise auto juhiga agressiivselt. Video autor avaldas selle video oma sotsiaalmeediakontol, mida jagati edasi ning mille lõpuks meedia ka päevakorraale võttis. Video on väga hea kvaliteediga ning sellelt on selgelt näha nii andmesubjekt kui ka tema auto ja auto registreerimisnumber. Isik on salvestiselt otseselt tuvastatav. Võib tekkida küsimus, et kas antud juhul andmesubjekti tundmatuse ni hägustamata jätmine on õigustatud. Autor on antud juhtumi puhul seisukohal, et andmesubjekti hägustamine ei ole põhjendatud, kuna päris kindlasti esineb liikluses vägivaldselt või ähvardavalt käituva isiku suhtes avalik huvi. Igaühel on õigus teada, kes on teistele ja seab teisi liikluses ohtu<sup>98</sup>. Ühtlasi leiab autor, et video avaldamine sellisel kujul ei lähe vastuollu ajakirjanduseetikaga, kuna videol on näha kogu sündmuse kõik algusest lõpuni. Kui videost oleks avaldatud ainult lõik, kus autost väljub kurikaga mees ja videost ei oleks võimalik tuvastada, mis antud olukorra põhjustas, siis ei tohiks täpseid fakte teadmata autori hinnangul isikuandmeid avaldada. Ühtlasi ei ole antud loo konteksti arvestades tegemist andmesubjekti õiguste ülemäärase kahjustamisega, seega on sellisel kujul video levitamine autori hinnangul õigustatud.

Kokkuvõtvalt ei saa andmetöötajat võtta vastutusele ja andmetöötaja võib salvestise avaldada ajakirjanduslikul eesmärgil, kui korraga esinevad järgmised kolm tingimust: esineb ülekaalukas avalik huvi, avaldamine on kooskõlas ajakirjanduseetika põhimõtetega ning ei kahjustata ülemäära andmesubjekti õigusi<sup>99</sup>. Enamasti kehtivad eelpool nimetatud kolm tingimust avaliku elu tegelase puhul, kes on pidanud arvestama, et tema vastu on kõrgendatud avalikkuse tähelepanu. Kui kasvõi üks kolmest tingimusest ei ole täidetud, siis salvestise avaldamine ilma andmesubjekti nõusolekuta ei ole lubatud ning avaldamise korral on võimalik andmetöötaja võtta vastutusele.

---

<sup>97</sup> Delfi.ee. VIDEO: Liiklusraev ja võõraviha Tallinnas: ohtliku olukorra tekitanud mees peatas keset teed auto ja ähvardas järelsõitjat kurikaga. [www.delfi.ee/news/paevauudised/krimi/video-liiklusraev-ja-vooraviha-tallinnas-ohtliku-olukorra-tekitanud-mees-peatas-keset-teed-auto-ja-ahvardas-jarelsoitjat-kurikaga?id=74476625](http://www.delfi.ee/news/paevauudised/krimi/video-liiklusraev-ja-vooraviha-tallinnas-ohtliku-olukorra-tekitanud-mees-peatas-keset-teed-auto-ja-ahvardas-jarelsoitjat-kurikaga?id=74476625) (27.04.2017)

<sup>98</sup> Tammer, *supra* nota 17, lk 657.

<sup>99</sup> IKS, *supra* nota 14, § 11, lg 2.

#### 1.4.1.3 Avaldamine asutusele, kes töötleb isikuandmeid seaduses sätestatud ülesande täitmiseks

IKS võimaldab nõusolekuta salvestise avaldada kolmandatele isikutele, kui kolmas isik, kellele andmed edastatakse, töötleb isikuandmeid seaduse, välislepingu või Euroopa Liidu Nõukogu või Euroopa Komisjoni otsekohalduva õigusaktiga ettenähtud ülesande täitmiseks<sup>100</sup>. Siia alla liigitub näiteks politseile video avaldamine, kui kaamera salvestisele on jäänud mõni süütegu ja see oleks oluliseks abiks ja tõendiks süüteo menetlemisel<sup>101</sup>.

Näiteks kui auto pardakaamera videole jääb juhtum, kus kahe autojuhi vahel on tekkinud konflikt ja üks neist kakkuse käigus raskelt viga saab, võiks politseil olla sellisest materjalist palju abi. Seda eriti olukorras, kus kannatanu avalduse esitab ning asja lahendamiseks on oluline tõendite olemasolu. Seni, kuni salvestis edastatakse ainult politseile ja ei avaldata mujal ega edastata muudele kolmandatele isikutele, ei saa andmetöötlejat andmete avaldamise eest vastutusele võtta.

#### 1.4.1.4 Avaldamise eesmärgil salvestamine

Kui andmetöötleja soovib avalikus kohas salvestada ning mitte enda tarbeks, vaid plaanibki materjali avaldada, siis jätab IKS selleks võimaluse. Korrakaitseseaduse<sup>102</sup> (KorS) § 54 defineerib avalikku kohta kui määratlemata isikute ringile kasutamiseks antud või määratlemata isikute ringi kasutuses olevat maa-ala, ehitist, ruumi või selle osa, samuti ühissõidukit. Loomulikult võib avalikus kohas viibida palju inimesi ja igapäevast nõusoleku saamine oleks mõeldamatu, seega avalikus kohas salvestamise korral avaldamise eesmärgil saab andmesubjekti nõusolekut asendada teavitamine sellises vormis, mis võimaldab andmesubjektil jäädvustamise faktist aru saada ning vajadusel seda vältida<sup>103</sup>. Selline teavitamiskohustus kehtib aga ainult sellisel juhul, kui tegemist ei ole avaliku üritusega, kus võib mõistlikult jäädvustamist eeldada<sup>104</sup>. KorS<sup>105</sup> § 58 lg 3 mõistes on avalik üritus avalikus kohas toimuv ja avalikkusele avatud lõbustusüritus, võistlus, etendus, kaubandusüritus või muu sellesarnane inimeste koos olemine, mis ei ole koosolek. Ehk siis avalikul üritusel salvestamisel avaldamise eesmärgil võib andmetöötleja ainult eeldada, et tal on

<sup>100</sup> IKS, *supra* nota 14, § 14, lg 2, p 1.

<sup>101</sup> Andmekaitse Inspeksioon (2016), *supra* nota 21, lk 7; Aleksejeva, *supra* nota 83, lk 45.

<sup>102</sup> KorS RT I, 02.12.2016, 6.

<sup>103</sup> IKS, *supra* nota 14, § 11, lg 8.

<sup>104</sup> *Ibid.*

<sup>105</sup> KorS, *supra* nota 102.

isikute nõusolek. Eeldust võib andmesubjekt igal ajal murda ja keelata enda kujutise avalikustamine<sup>106</sup>.

Auto pardakaamera puhul on ülal toodud nõudmisi ilmselt keeruline täita. Autori arvates pole levinud praktika, et autole näiteks kõikidele nähtavaid silte kleebitakse eesmärgiga teavitada, et toimumas on avaldamise eesmärgil salvestamine ning niimoodi ringi sõidetakse. Lisaks oleks inimesel väga keeruline liikuva auto salvestisele jäämist raske vältida isegi, kui ta antud teavitust näeks<sup>107</sup>. Avalikus kohas on inimesel pigem võimatu salvestisele jäämist vältida ning seega tuleb saada andmete töötlejal igalt isikult nõusolek või katta salvestisel isikud selliselt, et nad ei ole tuvastatavad<sup>108</sup>. Teavitamise kohustus langeb ära, kui sõita töötava pardakaameraga avaliku ürituse territooriumil ja hiljem see avaldada. Andmetöötlejal tuleks aga arvestada, et hiljem võivad avalikul üritusel pardakaamera ette jäänud inimesed lasta ennast antud salvestiselt eemaldada.

Sellest tulenevalt saab järeldada, et vastutuse vältimiseks tuleks avalikus kohas salvestamisel ja materjali hilisemal avaldamisel veenduda, et salvestisel ei oleks äratuntavaid isikuid. Avalikul üritusel salvestatud materjali avaldamisel ei ole andmetöötleja kohustatud salvestisel olevaid isikuid kuidagi varjama ning avaldamisega ei kaasne ka vastutust, kuid andmesubjekti nõudmisel peab andmetöötleja andmesubjekti tundmatuks muutma.

## 1.4.2 Juhud, kus isikuandmete avaldamine on keelatud

### 1.4.2.1 Andmesubjekt äratuntav ja nõusolek puudub

IKS sätestab, et isikuandmeid võib töödelda ainult kas seaduse alusel või isiku nõusolekul<sup>109</sup>, kuid jätab võimaluse töödelda isikuandmeid ka nõusolekuta, kui neid töödeldakse:

- 1) seaduse alusel;
- 2) välislepingu või Euroopa Liidu Nõukogu või Euroopa Komisjoni otsekohalduva õigusaktiga ettenähtud ülesande täitmiseks;
- 3) üksikjuhtumil andmesubjekti või muu isiku elu, tervise või vabaduse kaitseks, kui andmesubjektilt ei ole võimalik nõusolekut saada;

---

<sup>106</sup> Tammer, *supra* nota 17, lk 656.

<sup>107</sup> Andmekaitse Inspektsioon (2016), *supra* nota 21, lk 9.

<sup>108</sup> *Ibid.*

<sup>109</sup> IKS, *supra* nota 14, § 10, lg1.

4) andmesubjektiga sõlmitud lepingu täitmiseks või lepingu täitmise tagamiseks, välja arvatud delikaatsete isikuandmete töötlemine<sup>110</sup>.

IKS eristab veel isikuandmete edastamist ja juurdepääsu võimaldamist, mis on nõusolekuta lubatud:

- 1) kui kolmas isik, kellele andmed edastatakse, töötleb isikuandmeid seaduse, välislepingu või Euroopa Liidu Nõukogu või Euroopa Komisjoni otsekohalduva õigusaktiga ettenähtud ülesande täitmiseks;
- 2) üksikjuhtumil andmesubjekti või muu isiku elu, tervise või vabaduse kaitseks, kui andmesubjektilt ei ole võimalik nõusolekut saada;
- 3) kui kolmas isik taotleb teavet, mis on saadud või loodud seaduses või selle alusel antud õigusaktides sätestatud avalikke ülesandeid täites ja taotletav teave ei sisalda delikaatseid isikuandmeid ning sellele ei ole muul põhjusel kehtestatud juurdepääsupiirangut<sup>111</sup>.

Salvestise avaldamine, edastamine ja kolmandatele isikutele juurdepääsu võimaldamine on keelatud, kui vastavad nõuded ei ole täidetud. Kõige tõenäolisemad juhtumid auto pardakaamerate puhul, kus nõusolekuta võiks salvestise avaldada laskuvad ilmselt üksikjuhtumite kategooriasse, kui salvestis avaldatakse andmesubjekti või muu isiku elu, tervise või vabaduse kaitseks. Näiteks kui peaks pardakaamera salvestisele jääma tänaval toimuv rööv ning röövi toime pannud isiku põgenemine ja millel on selgelt näha isiku nägu. Antud salvestis tuleks kindlasti kiiresti avaldada eelkõige teiste isikute kaitseks ja video avaldamine kaalub kindlasti üle röövi toime pannud isiku õigused.

Tihti aga avaldavad andmete töötlejad just teadmatuses salvestise pööramata tähelepanu, kas salvestisel on äratuntavaid isikuid ning isiku identifitseeritavuse risk lasub täielikult andmetöötlejal<sup>112</sup>. Kui salvestis on siiski avaldatud ning salvestisel on äratuntavad isikud, kes ei ole nõusolekut andnud, on andmesubjektidel õigus nõuda isikuandmete töötlemise lõpetamist<sup>113</sup>. Esmajärjekorras tuleks andmete töötlemise lõpetamist nõuda andmete töötlejalt ning kui see ei too tulemust on andmesubjektidel õigus pöörduda Andmekaitse Inspektsiooni või kohtu poole<sup>114</sup>. Pärast

---

<sup>110</sup> *Ibid*, § 14, lg 1.

<sup>111</sup> *Ibid*, § 14, lg 2.

<sup>112</sup> Tikk, Nõmper, *supra* nota 11, lk 50.

<sup>113</sup> IKS, *supra* nota 14, § 21, lg 2.

<sup>114</sup> Andmekaitse Inspektsioon (2016), *supra* nota 21, lk 30; IKS, *supra* nota 14, § 22.

vastavat taotlust on andmete töötlejal kohustus viivitamatult vastav toiming teha ning andmesubjekti tuleb toimingu rahuldamisest või rahuldamata jätmisest ka teavitada<sup>115</sup>.

## 1.5 Isiku tuvastamine

### 1.5.1 Isiku kaudne tuvastamine

Autor käsitles alapeatükis 1.1, et IKS § 4 lg 1 defineerib isikuandmeid kui mis tahes andmeid tuvastatud või tuvastamata füüsilise isiku kohta ning nende vorm ei ole oluline<sup>116</sup>. See tähendab, et näiteks isegi isiku kujutis liigitub isikuandmete alla<sup>117</sup>. Kujutis on miski, mille kaudu ühiskond tunneb meid ära ja eristab<sup>118</sup>. Isiku tuvastatavuse hindamisel tuleb võtta arvesse kõiki asjaolusid, mille alusel isik võib tuvastatav olla ning seejuures ei ole oluline, kas isik on tuvastatav üldiste omaduste või konteksti põhjal<sup>119</sup>. Seega alati ei piisa isegi isiku näo varjamisest salvestisel, sest isik võib olla endiselt äratuntav mõne tema muu iseäraliku tunnuse järgi. Seda kinnitab veelkord ka Riigikohus, kes on leidnud, et isiku kujutist on lubatud kasutada, kui see on tehniliste vahenditega muudetud selliseks, mis ei võimalda isikut tuvastada<sup>120</sup>. Muudatus peaks olema selliselt teostatud, et ei oleks võimalik isikut tuvastada ka konteksti alusel<sup>121</sup>. Suhteliselt värskes otsuses leiab Euroopa Kohus, et Liidu seadusandja poolt sõna „kaudselt“ kasutamise soovitakse näidata, et isikuandmeteks määratlemiseks ei pea need andmed ise võimaldama kõnealust isikut tuvastada<sup>122</sup>. Näiteks mõistmaks, kui laialt on võimalik isikuandmeid käsitleda, siis samas otsuses leidis Euroopa Kohus, et isikuandmeteks kvalifitseerub ka dünaamiline IP-aadress, kui selle teeb teenusepakkuja üldsusele kättesaadavaks<sup>123</sup>.

AKI seisukoht on, et auto pardakaamera salvestisele jäänud autodes istuvad inimesed tuleb salvestisel avaldamise korral hägustada, kuid näiteks auto ise ja selle numbrimärk isikuandmete alla ei kuulu<sup>124</sup>. Põhjuseks toob AKI, et ei ole võimalik teha ühest järeldust, kes sellel hetkel autoga liikles ning ühe autoga võib sõita mitu erinevat inimest, küll aga soovitab sõltuvalt salvestise

---

<sup>115</sup> Isikuandmete kaitse seaduse eelnõu seletuskiri, *supra* nota 79, § 21.

<sup>116</sup> IKS, *supra* nota 14, § 4, lg 1.

<sup>117</sup> RKTko 3-2-1-159-14, p 13.

<sup>118</sup> Tammer, *supra* nota 17, lk 652.

<sup>119</sup> Isikuandmete kaitse seaduse eelnõu seletuskiri, *supra* nota 79, § 4.

<sup>120</sup> RKTko 3-2-1-152-09, p 14.

<sup>121</sup> *Ibid.*

<sup>122</sup> EKO 19.10.2016, C-582/14, *Breyer vs Saksamaa Liitvabariik*, p 41.

<sup>123</sup> *Ibid.*, p 49.

<sup>124</sup> Andmekaitse Inspeksioon (2016), *supra* nota 21, lk 9.

kontekstist kaaluda numbrimärkide hägustamist<sup>125</sup>. Artikli 29 alusel asutatud andmekaitse töörihm on avaldanud arvamust, et auto numbri alusel on isik kaudselt tuvastatav<sup>126</sup>. Autor on AKI seisukohaga päri, et auto numbrimärgid ei vaja hägustamist, kui sõiduk osaleb igapäevases liikluses, kuid vajaksid kindlasti hägustamist, kui sõiduk on pargitud. Salvestisel näha olev pargitud sõiduk kindla asutuse ees võib anda sõiduki omaniku sõpradele ja tuttavatele, kes auto ära tunnevad, põhjust oletusteks ja avaldada neile isikuandmeid, mida isik ise võib-olla avaldada ei soovi. Avalikuks võivad saada sellisel viisil ka delikaatsed isikuandmed, milleks on IKS § 4 lg-s 2 toodud andmed, kui näiteks andmesubjekti auto pargib eriarsti parklas. Sellisel viisil delikaatsete isikuandmete avaldamine liigitub autori hinnangul isiku õiguste ülemäärase kahjustamise alla.

Autori hinnangul on kaudselt tuvastatavad ka kõik isikud, kes sõidavad reklaame kandvate autodega. Mida vähem liigub sarnaste reklaamkleebistega autosid, seda paremini on võimalik isik kaudselt tuvastada. Siia alla kuuluvad näiteks väiksemate ettevõtete autod, kus võib-olla on reklaamkleebistega autosid üks või kaks. On ka selliseid reklaamkleebistega autosid, kus on autol ära toodud isikute nimed. Avaldamisele kuuluval salvestisel tuleks kõik see hägustada, kui puudub õiguslik alus isikuandmete avaldamiseks.

Kaudne tuvastamine ei pruugi olla niivõrd hõlpsalt võimalik suurfirmade reklaame kandvate autode puhul nagu Eesti kontekstis näiteks Saku, Telia, Starman ettevõtete puhul, kus sarnase kujundusega autosid liigub võib-olla sadu. Ühtlasi liigub ka rendiautosid, millel on rendifirma reklaamkleebised – ka sellisel juhul ei ole autori hinnangul isik sõidukis väljast vaadatuna otseselt ega kaudselt tuvastav, kui just tema nägu selgelt nähtav ei ole.

Eelnevast tuleneb, et alati ei pruugi isik kaudselt tuvastatav olla konkreetse ühe näitaja põhjal, vaid pigem on oluline mitme näitaja kombinatsioon ning igas olukorras tuleb andmeid hinnata erinevalt<sup>127</sup>.

---

<sup>125</sup> *Ibid.*

<sup>126</sup> Article 29 Data Protection Working Party. Opinion 4/2007 on the concept of personal data, 2007. [www.clinicalstudydatarequest.com/Documents/Privacy-European-guidance.pdf](http://www.clinicalstudydatarequest.com/Documents/Privacy-European-guidance.pdf) (24.04.2017), lk 13.

<sup>127</sup> *Ibid.*

## 1.5.2 Isiku otsene tuvastamine

Euroopa Liidu isikuandmete kaitse üldmäärus sätestab, et tuvastatav füüsiline isik on isik, keda saab otseselt või kaudselt tuvastada, eelkõige sellise identifitseerimistunnuse põhjal nagu nimi, isikukood, asukohateave, võrguidentifikaator või selle füüsilise isiku ühe või mitme füüsilise, füsioloogilise, geneetilise, vaimse, majandusliku, kultuurilise või sotsiaalse tunnuse põhjal<sup>128</sup>. Ei IKS ega ka Euroopa Liidu andmekaitse üldmäärus ei defineeri ega anna ammendavat nimekirja, mis on otsese tuvastamise tunnused. Euroopa Nõukogu on välja toonud, et tuvastamine ei tohi nõuda andmete töötlemist erimeetmete ega -vahenditega ehk isik peab olema kergesti äratuntav ning tuvastatavuse üle tuleb otsustada lähtudes sellele kulunud ajast, kulukusest ja inimressursist<sup>129</sup>.

Isiku võib tuvastada otseselt nime alusel<sup>130</sup>. Seega isik on otseselt tuvastatav, kui mingil viisil on salvestisel nähtav tema nimi. Seda näiteks olukorras, kus isik kannab mingil põhjusel rinnas nimesilti ja see on jäänud salvestisele loetavalt näha. Nähtava nimesildi puhul võib levinud nime korral osutada otsene tuvastamine ka keeruliseks, kuna on vähetõenäoline, et nimesildil on ka isiku isikukood, mis on levinud nimede puhul on üks tuvastamise vahenditest. Olenevalt salvestise sisust võib ka levinud nimega isik olla konteksti põhjal otseselt tuvastatav. Kindlasti on otseselt tuvastatav ka näiteks sportlane, kelle spordiriietele on suurelt tema nimi märgitud. Siia alla ei kvalifitseeru olukord, kus salvestisele jääb isik, kes kannab näiteks jalgpallisärki, mille seljal on suurelt kuulsa jalgpalluri nimi, kuid andmetöötleja peaks ise veenduma, kas tegemist on fänniga või reaalse sportlasega, kes kannabki oma nimega riietust. Autori arvamus on, et isik on kindlasti otseselt tuvastatav ka olukorras, kus selgelt on jäänud salvestisele näha tema nägu. Kõik muud olukorrad kvalifitseeruvad pigem isiku kaudse tuvastamise valdkonda.

Kokkuvõtvalt peaks iga andmetöötleja sõltuvalt oma salvestise eripärast enne salvestise avaldamist veenduma, kas lisaks otsesele tuvastamisele on tema salvestisel võimalik kedagi ka kaudselt tuvastada. Kaudne tuvastamine on võimalik, kui kombineerida üks või mitu näitajat ning otseselt on isik tuvastatav, kui on nähtav tema nimi või nägu. Vähimagi kahtluse korral, kas keegi on otseselt või kaudselt salvestisel tuvastatav ning kui nõusoleku saamine on välistatud, tuleks

<sup>128</sup> OJ L 119, 04.05.2016, art 4 p 1.

<sup>129</sup> Tikk, Nõmper, *supra* nota 11, lk 80.

<sup>130</sup> Article 29 Data Protection Working Party, *supra* nota 126, lk 12.

vastavad kohad kinni katta või tundmatuseni hägustada. Muidugi tuleb läheneda probleemile ka ratsionaalselt ja näiteks olukorras, kus salvestisel on igapäevane liiklus, siis auto registreerimisnumbreid ja reklaamkleebiseid autori hinnangul hägustama ei peaks. Küll aga peaks autori hinnangul hägustama parkivate sõidukite andmed, sest kaudse tuvastamise kaudu võivad sellisel viisil avalikuks saada näiteks isiku elukoht või arsti juures käik (nt eriarsti parklas asuvate autode kaameraga jäädvustamine) ning näiteks viimane kvalifitseerub juba delikaatsete isikuandmete alla<sup>131</sup>.

## 1.6 Vastutus

Igapäevane internetikasutaja ei pruugi aimatagi, et teatud andmete üleslaadimisel Internetti võib talle tekkida reaalne vastutus ja järgneda ka karistus. Parimal juhul palub andmesubjekt otse töötlejal materjal avalikkuse silmade eest eemaldada. Halvimal juhul peavad sekkuma kolmandad isikud. Järgnevalt analüüsib autor, millistel juhtudel ja milline vastutus ja sanktsioonid on võimalikud, kui teadmatuses või teadlikult on avaldatud kellegi isikuandmeid.

### 1.6.1 Vastutust välistavad asjaolud

Vastutusele ei ole võimalik võtta andmetöötlejat, kes täidab seadust ja ei ole kellegi õigusi rikkunud. Andmetöötlejat ei ole võimalik võtta vastutusele, kui ta salvestab oma auto pardakaameraga isiklikuks otstarbeks, millest autor on kirjutanud eelnevalt alapeatükis 1.3. Ühtlasi peab salvestisi säilitama viisil, et neile ei oleks ligipääsu kolmandatel isikutel (ei oma tähtsust see, kastegeemist on arvutiga, välise kõvaketta või pilveteenusega).

Vastutuse välistab ka olukord, kui salvestisel otseselt või kaudselt äratuntavalt inimestelt on andmetöötlejal olemas nõusolek salvestise avaldamiseks<sup>132</sup> või mõni muu õiguslik alus isikuandmete töötlemiseks. Andmesubjekt võib igal ajal oma nõusoleku tagasi võtta, mis tähendab, et ka andmetöötleja peab salvestise koheselt avalikkusest eemaldama. Nõusoleku tagasivõtmisel ei ole tagasiulatuvaid tagajärgi<sup>133</sup>. Andmesubjekt ei saa eeldada, et nõusoleku

---

<sup>131</sup> IKS, *supra* nota 14, § 4, lg 2.

<sup>132</sup> Vt alapunkt 1.4.1.1

<sup>133</sup> Andmekaitse Inspeksioon (2016), *supra* nota 21, lk 20; IKS, *supra* nota 14, § 12, lg 7.

tagasivõtmisel kaob juba levima hakanud pardakaamera salvestis tervest Internetist, sest eriti kiiresti levivad kõik vähegi huvitavad materjalid just sotsiaalmeedias ning andmetöötaja poolt salvestise eemaldamisest ei pruugi enam piisata. Andmesubjekt ei saa nõuda töötlejalt avalikustamise lõpetamist selliste materjalide suhtes, mille üle puudub töötlejal otsene kontroll<sup>134</sup>, kuid saab seda nõuda ka vastutavatelt töötajatelt nagu näiteks otsingumootorid. 2014. aastal lõi Euroopa Kohus *Google Spain* otsuses õiguse olla unustatud<sup>135</sup>. See tähendab, et andmesubjektil on õigus otsingumootori haldajalt nõuda isikuandmeid sisaldava teabe eemaldamist, kui tema õigus eraelule ja andmekaitsele kaalub üles üldsuse huvi teabe saamise vastu<sup>136</sup>. Õigust andmete kustutamisele reguleerib ka isikuandmete kaitse üldmäärus<sup>137</sup>, mis annab õiguse andmete kustutamisele järgnevatel juhtudel:

- 1) isikuandmeid ei ole enam vaja sellel eesmärgil, millega seoses need on kogutud või muul viisil töödeldud;
- 2) andmesubjekt võtab töötlemiseks antud nõusoleku tagasi ning puudub muu õiguslik alus isikuandmete töötlemiseks;
- 3) andmesubjekt esitab vastuväite isikuandmete töötlemise suhtes ja töötlemiseks pole ülekaalukaid õiguspäraseid põhjuseid;
- 4) isikuandmeid on töödeldud ebaseaduslikult;
- 5) isikuandmed tuleb kustutada selleks, et täita vastutava töötleja suhtes kohaldatava liidu või liikmesriigi õigusega ette nähtud juriidilist kohustust;
- 6) isikuandmeid koguti seoses artikli 8 lõikes 1 osutatud infoühiskonna teenuste pakkumisega.

Sellest tulenevalt võib järeldada, et kui andmesubjekt võtab tagasi nõusoleku salvestise avaldamiseks, siis on tal õigus nõuda salvestise eemaldamist nii salvestise avaldajalt kui ka muudelt vastutavatelt töötajatelt nagu näiteks otsingumootoritelt.

Kui salvestis on avaldatud avalikes huvides ja ajakirjanduslikul eesmärgil peavad olema vastutuse vältimiseks täidetud kolm eeldust: ülekaalukas avalik huvi, salvestis on kooskõlas ajakirjanduseetika põhimõtetega ning ei kahjustata liigselt andmesubjekti õigusi<sup>138</sup>. Kõik need

---

<sup>134</sup> Andmekaitse Inspeksioon (2016), *supra* nota 21, lk 29; IKS, *supra* nota 14, § 11, lg 3.

<sup>135</sup> EKo 13.05.2014, C-131/12, *Google Spain SL, Google Inc. v. Agencia de Protección de Datos (AEPD), Mario Costeja González*.

<sup>136</sup> Tupay, *supra* nota 38, lk 233; *Ibid*, p 99.

<sup>137</sup> OJ L 119, 04.05.2016, art 17, lg 1.

<sup>138</sup> Vt alapunkt 1.4.1.2

kolm tingimust peavad olema täidetud korraga<sup>139</sup>. Enamasti kehtivad need tingimused avaliku elu tegelase puhul, seega andmetöötaja peaks vastutuse vältimiseks väga hoolega kaaluma, kas kõik eelpool mainitud 3 tingimust on täidetud.

Kokkuvõtvalt tuleb vastutuse vältimiseks eelkõige hoolega süveneda avaldamisele mineva salvestise sisusse. Kui salvestisel on äratuntavad isikud, siis tuleb neilt saada nõusolekud (või peab eksisteerima mõni muu alus isikuandmete töötlemiseks) või tundmatuseni kinni katta või hägustada ning seeläbi muuta isikud mitteidentifitseeritavaks.

## 1.6.2 Haldusvastutus

Eestis teostab IKSis sätestatud nõuete täitmise üle riiklikku ja haldusjärelvalvet AKI<sup>140</sup>. AKI kontrollib IKSis sätestatud nõuete täitmist, rakendab seadustes ettenähtud alustel, ulatuses ja korras haldussundi, algatab vajaduse korral väärteomenetluse ja kohaldab karistust, annab soovituslikke juhiseid IKS-i rakendamiseks ning täidab muid seadustest tulenevaid ülesandeid<sup>141</sup>. AKI-l on õigus peatada isikuandmete töötlemine, nõuda ebaõigete isikuandmete parandamist, keelata isikuandmete töötlemine, nõuda isikuandmete sulgemist või töötlemise lõpetamist, sealhulgas hävitamist või edastamist arhiivi, rakendada isiku õiguste ja vabaduste kahjustamise ärahoidmiseks vajaduse korral asendustäitmise ja sunniraha<sup>142</sup>. Seega AKI ei lahenda isikute vahelisi vaidlusi ega mõista kelleltki välja kahjuhüvitusi<sup>143</sup>.

AKI ei sekku eraisikute vahelisse vaidlusse enne, kui andmesubjekt on juba pöördunud andmetöötaja poole ning soovinud avalikustamise lõpetamist, kuid seda ei ole andmetöötaja poolt tehtud<sup>144</sup>. Kui andmetöötaja avalikustamist ei lõpeta, on andmesubjektil võimalus pöörduda AKI poole, kui olukord nõuab kiiremat tegutsemist, kui tsiviilkohtumenetlus seda võimaldaks<sup>145</sup>. Näiteks siia kuulukski olukord on salvestis ringleb sotsiaalmeedias ja Internetis kiiresti ning hilisem sekkumine oleks mõttetu<sup>146</sup>.

<sup>139</sup> Andmekaitse Inspeksioon (2016), *supra* nota 21, lk 15; RKTko 3-2-1-159-14, p 14.

<sup>140</sup> IKS, *supra* nota 14, § 32, lg 1.

<sup>141</sup> *Ibid*, § 33, lg 1.

<sup>142</sup> *Ibid*, § 33, lg 2.

<sup>143</sup> Andmekaitse Inspeksioon (2016), *supra* nota 21, lk 30.

<sup>144</sup> *Ibid*.

<sup>145</sup> *Ibid*; KorS, *supra* nota 102, § 4, lg 2.

<sup>146</sup> Andmekaitse Inspeksioon. Isikuandmete avalikustamine meedias: Andmekaitse Inspeksiooni sekkumiskriteeriumid, 2015.

Suure tõenäosusega võtab AKI menetlusse lisaks juhtumid, kus:

- andmesubjekt on abitus või eriliselt haavatavas seisundis ning tal ei ole võimalik oma õigusi kaitsa;
- avaldatud on alaealise isikuandmed;
- tegemist on delikaatsete isikuandmetega;
- rikkumine on korduv või puudutab suurt hulka inimesi;
- avalikustatakse raske õigusrikkumise teel saadud andmeid või on avalikustamine ise raske õigusrikkumine<sup>147</sup>.

AKI ei sekku järgnevatel juhtudel:

- avaldatakse avaliku elu tegelaste andmeid;
- andmesubjekt on kurjategija, kahtlusalune või süüdistatav;
- avaldatud on isiku ettevõtluse või kutsetegevuse või muu avalikkusele suunatud tegevusega seotud andmed;
- vaidlus käib andmete õigsuse üle, sh au ja hea nime teotamise ning laimusüüdistused;
- andmed on avaldatud väljaandes, mida pole võimalik tagantjärele vaadata/kuulata;
- andmeid ei ole veel avalikustatud;
- poolte vahel on käimas samal teemal kohtuvaidlus või vaidlus tsiviilõigusliku lepingu üle;
- andmesubjekt ise on andmed avalikustanud<sup>148</sup>.

Seega kui AKI võtabki andmesubjekti taotluse menetlusse, saab AKI nõuda andmetöötlejalt avaldamise lõpetamist, teha ettekirjutusi ning määrata sunniraha, sealhulgas korduvalt<sup>149</sup>. Reeglina alustab AKI haldusmenetlust haldusmenetluse seaduse<sup>150</sup> (HMS) § 35 ning IKS § 33 alusel<sup>151</sup>. Ettekirjutuse mittetäitmisel on AKI-l õigus rakendada andmetöötleja suhtes sunniraha, mille ülemmäär on 9600 eurot<sup>152</sup>. AKI tegi 2015. aastal 77 ettekirjutust, mis sisaldasid peaaegu alati

---

[www.aki.ee/sites/www.aki.ee/files/elfinder/article\\_files/Juhised/meediavaidluse%20sekkumise%20kriteeriumid.pdf](http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/Juhised/meediavaidluse%20sekkumise%20kriteeriumid.pdf) (05.03.2017), lk 2.

<sup>147</sup> *Ibid.*

<sup>148</sup> Andmekaitse Inspeksioon (2015), *supra* nota 146, lk 3.

<sup>149</sup> Andmekaitse Inspeksioon (2016), *supra* nota 21, lk 30.

<sup>150</sup> HMS RT I, 25.10.2016, 5.

<sup>151</sup> Sillaots, S. Isikuandmete kaitse regulatsiooni ühtlustamine isikuandmete kaitse üldmääruse eelnõus ja selle mõju Eestile, magistritöö, Tartu Ülikooli Õigusteaduskond 2014, lk 62.

<sup>152</sup> IKS, *supra* nota 14, § 40, lg 2.

kohe ka sunniraha-hoiatust ning reeglina kõik ettekirjutused täideti<sup>153</sup>. 2016. aastal tehti ettekirjutusi 59<sup>154</sup>. Ei ole teada, kui suur osa ettekirjutustest puudutas isikuandmete avaldamist, kuid 2015. aastal tegi AKI teoks ainult ühe sunniraha-ähvarduse<sup>155</sup>. See näitab autori hinnangul, et pigem ei ole rikkumised pahatahtlikud ning tulenevad teadmatusesest ja AKI reageerimise peale andmetöötledajad ka teevad enda poolt kõik, et rikkumine lõpetada. Eestis on sunniraha mõjutusvahend, mitte karistus<sup>156</sup>. Seega on andmetöötledaja haldusvastutus piirdunud üldiselt kas ettekirjutuse või sunnirahaga.

Kui tegemist on delikaatsete isikuandmetega, on AKI-l õigus alustada ka vääртеomenetlust, mille rahatrahvi suurus on kuni 300 trahviühikut<sup>157</sup>. Trahviühiku suurus on 4 eurot<sup>158</sup>, seega maksimaalne rahatrahv oleks 1200 eurot. Lisaks rahatrahvile kantakse andmetöötledaja sellisel juhul ka karistusregistrisse, mis on ka avalik<sup>159</sup>. Ei ole veel teada, kas karistusregister jääb avalikuks seoses isikuandmete kaitse üldmääruse<sup>160</sup> kehtima hakkamisega, kuid AKI peadirektor on seisukohal, et karistusregister peaks säilitama oma avatuse ning selleks tuleb välja mõelda head põhjendused<sup>161</sup>.

Kui andmesubjekt või andmetöötledaja ei ole AKI lahendusega nõus, siis on mõlemal poolel võimalik alustada vaidemenetlus 30 päeva jooksul<sup>162</sup>. Vaidemenetluse käigus võivad pooled nõuda haldusakti kehtetuks tunnistamist, selle mingi osa kehtetuks tunnistamist, ettekirjutuse tegemist haldusakti andmiseks ja asja uueks otsustamiseks või toimingute sooritamiseks<sup>163</sup>. Vaie tuleb esitada AKI üle teenistuslikku järelevalvet teostavale haldusorganile, ehk Justiitsministeeriumile<sup>164</sup>.

---

<sup>153</sup> Andmekaitse Inspeksioon. Avaliku teabe seaduse ja isikuandmete kaitse seaduse täitmisest aastal 2015. Soovitused aastaks 2016, 2016. [www.aki.ee/sites/www.aki.ee/files/elfinder/article\\_files/AASTARAAMAT.pdf](http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/AASTARAAMAT.pdf) (05.03.2017), lk 8.

<sup>154</sup> Andmekaitse Inspeksioon (2017), *supra* nota 5, lk 8.

<sup>155</sup> *Ibid.*

<sup>156</sup> Sillaots, *supra* nota 151, lk 64; RKÜKo 3-2-1-4-13, p 17.

<sup>157</sup> IKS, *supra* nota 14, § 42, lg 1.

<sup>158</sup> KarS RT I, 31.12.2016, 14, § 47, lg 1.

<sup>159</sup> Sootak, J. Karistusõiguse revisjon kuriteo-, vääртеo- ja haldusõiguse piirimail. *Juridica* IV/2013, lk 247; KarRS RT I, 30.12.2015, 17, § 6, lg 2.

<sup>160</sup> OJ L 119, 04.05.2016, art 10.

<sup>161</sup> Andmekaitse Inspeksioon. Andmekaitse Inspeksiooni peadirektori ülevaade andmekaitse reformi rakendamise seisust Eestis 14.10.2016, 2016. [www.aki.ee/sites/www.aki.ee/files/elfinder/article\\_files/ylevaade\\_reformist\\_14102016.pdf](http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/ylevaade_reformist_14102016.pdf) (09.04.2017), lk 5.

<sup>162</sup> HMS, *supra* nota 150, § 71, lg 1 ja § 75.

<sup>163</sup> *Ibid.*, § 72, lg 1.

<sup>164</sup> *Ibid.*, § 73, lg 1; Justiitsministeerium. Justiitsministeeriumi ja haldusala struktuur. [www.just.ee/et/ministeerium-kontaktid/ministeeriumi-tutvustus-ja-struktuur](http://www.just.ee/et/ministeerium-kontaktid/ministeeriumi-tutvustus-ja-struktuur) (05.03.2017).

Kokkuvõtvalt leiab kinnitust bakalaureusetöö hüpotees, et isiklikuks otstarbeks salvestatud auto pardakaamera video avaldamine võib kaasa tuua vastutuse. Ühtlasi leidis autor vastuse uurimisküsimusele, millised on isiklikuks otstarbeks salvestatud auto pardakaamera salvestise avaldamise võimalikud tagajärjed füüsilisest isikust avaldajale. Haldusmenetluse käigus võib andmetötleja suhtes rakendada ettekirjutusi, määrata korduvalt sunniraha maksimaalselt summas 9600 eurot ning alustada väärtemenetlust, milles on rahatrahvi suurus maksimaalselt 1200 eurot. Lisaks jääb väärtemenetlusest karistusregistrisse andmetötleja kohta sissekanne, millega on võimalik tutvuda igapäev, sest bakalaureusetöö kirjutamise hetkel on karistusregister veel avalik.

### 1.6.3 Tsiviilvastutus

Lisaks otse andmetötleja ja AKI poole pöördumisele on andmesubjektile oma õiguste kaitseks võimalik pöörduda ka kohtu poole, kui eelpool mainitud meetodid olukorda ei lahenda või kui näiteks AKI menetlust ei alusta. Üldiselt on isikuandmete rikkumiste puhul väga raske taastada rikkumisele eelnenud olukorda<sup>165</sup>. Mida laiemale publikule on salvestis kättesaadavaks saanud, seda suurem on kahju.

Vastavalt IKS § 23 p 2 on andmesubjektile õigus nõuda kahju hüvitamist eraõiguslikus suhtes rikutud õiguste korral võlaõigusseaduses<sup>166</sup> (VÕS) sätestatud alustel ja korras.

VÕS § 1046 lg 1 sätestab, et isiku au teotamine, muu hulgas ebakohase väärtushinnanguga, isiku nime või kujutise õigustamatu kasutamine, eraelu puutumatus või muu isikliku õiguse rikkumine on õigusvastane, kui seadusega ei ole sätestatud teisiti. Vastavalt VÕS § 128 lg-le 1 võib hüvitamisele kuuluv kahju olla kas varaline või mittevaraline. Kuna isikuandmete õigusvastane avaldamine põhjustab andmesubjektile eelkõige hingelist valu ja kannatusi, siis autori hinnangul on isikuandmete puhul hüvitatava kahju liigiks mittevaraline kahju VÕS § 128 lg 5 mõistes. Samale seisukohale on jäänud ka õiguskirjanduses<sup>167</sup>. Vastavalt VÕS § 134 lg 5 arvestatakse

---

<sup>165</sup> Männiko, M. Õigus privaatsusele ja andmekaitse. Tallinn, Juura 2011, lk 85.

<sup>166</sup> VÕS RT I, 06.01.2016, 10

<sup>167</sup> Tammer, *supra* nota 17, lk 661.

mittevaralise kahju hüvitise määramisel rikkumise raskust ja ulatust<sup>168</sup> ning kahju tekitaja käitumist ja suhtumist kahjustatud isikusse pärast rikkumist. Siinkohal võiks hüvitise summa määramisel raskendavaks asjaoluks muutuda andmetöötaja mittereageerimine andmesubjekti pöördumistele, näiteks salvestise eemaldatama jätmise sotsiaalmeediast ning ka selle salvestise edasine levitamine peale sellekohase märkuse saamist<sup>169</sup>. Mittevaralise kahju hüvitise korral on tegemist hinnangulise otsusega, mille suuruse otsustab vastavalt VÕS § 127 lg 6 kohus<sup>170</sup> ning arvesse tuleb võtta kõike, mis võib mõjutada hüvitise määra õiglast kujunemist kohtuasjas<sup>171</sup>.

Kui tegemist on olulise andmesubjekti õiguste riivega, on andmesubjektil õigus nõuda ebaseadusliku töötlemisega kaasneva moraalse kahju hüvitamist<sup>172</sup>. PS § 25 sätestab, et igal on õigus talle ükskõik kelle poolt õigusvastaselt tekitatud moraalse ja materiaalse kahju hüvitamisele. Siin tuleb aga rõhutada, et raha ei saa kõrvaldada mittevaralist kahju, sest valu ei ole võimalik rahaga ära võtta, see on üksnes kompensatsioon<sup>173</sup>. Seega on võimalik valuraha nõuda vaid juhul, kui muul viisil ei ole võimalik tekitatud kahju heastada<sup>174</sup>. Auto pardakaamera video avaldamise puhul tuleks autori hinnangul moraalse kahju hüvitamine kõne alla, kui salvestis on saanud väga suure tähelepanu osaliseks näiteks sotsiaalmeedias, mida lisaks on kajastanud ka meedia. Kui andmesubjekt on sellisel salvestisel kajastatud äratuntavalt ning ta ei ole selleks oma nõusolekut andnud, oleks autori hinnangul andmesubjektil õigus moraalse kahju hüvitamisele. Mittevaralise kahju rahalise hüvitise suuruse määrab kohus kindlaks oma siseveendumuse kohaselt kõiki asjaolusid arvestades ning selleks puuduvad objektiivsed kriteeriumid<sup>175</sup>. Arvesse tuleb võtta õiguse üldpõhimõtteid (sh võrdsus), ühiskonna üldist heaolu taset, kohtupraktikat, rikutud õiguse kaalukust ja „valu suurust“<sup>176</sup>.

Ka tsiviilvaidluste korral on salvestise avaldaja vastutusele võtmine võimalik ning kinnitust on saanud bakalaureusetöö hüpotees, et isiklikuks otstarbeks salvestatud auto pardakaamera video

---

<sup>168</sup> Näiteks toob Riigikohtu tsiviilkolleegium välja otsuse 3-2-1-18-13 p-s 28, et tuleb arvestada näiteks seda, kas artikkel avaldati üksnes paberväljaandes või lisaks ka Internetis, kus see jõuab eelduslikult oluliselt suurema hulga lugejateni kui paberväljaandes.

<sup>169</sup> Vt ka *Ibid.*, lk 662.

<sup>170</sup> Tampuu, T. Deliktiõigus võlaõigusseaduses. Üldprobleemid ja delikti üldkoosseisul põhinev vastutus. *Juridica* II/2003, lk 73.

<sup>171</sup> RKTko 3-2-1-18-13, p 28.

<sup>172</sup> Männiko, *supra* nota 165, lk 85.

<sup>173</sup> § 25, p 2.4.2. Põhiõigused, vabadused ja kohustused. II peatükk. Eesti Vabariigi põhiseadus. Kommenteeritud väljaanne. [www.pohiseadus.ee/ptk-2/pg-25/](http://www.pohiseadus.ee/ptk-2/pg-25/) (05.03.2017).

<sup>174</sup> *Ibid.*

<sup>175</sup> *Ibid.*

<sup>176</sup> *Ibid.*

avaldamine võib kaasa tuua vastutuse. Uurimisküsimusele saab vastata tsiviilõiguse poolelt vaadatuna, et andmetöötajale võidakse esitada mittevaralise või moraalse kahju hüvitamise nõue, mille suurus sõltub tagajärgede tõsidusest, ulatusest ja kohtu otsusest.

## 2. Auto pardakaameratele ja isikuandmete töötlemiseolukordadele kehtiva õigusraamistiku tulevik

On kindel, et auto pardakaamerate levik saab ühe hoogu juurde, kuna kaameratel on ka väga suur praktiline väärtus. Nimelt aitab see oluliselt lihtsustada menetlust liiklusõnnetuse korral eriti olukorras, kus kahe poole ütlused ei ühti. Kuna kahe liiklusõnnetusse sattunud isiku erimeelsuste korral kaasatakse peaaegu alati ka politsei, siis on õnnetuse menetluses videosalvestisel oluline koht. Mida rohkem on kaameraid, seda rohkem jääb nende kaamerate ette ka erinevaid sündmuseid, mida inimesed soovivad näiteks sotsiaalmeedias jagada. See kõik tähendab, et ka suurem hulk isikuandmeid võib sattuda õigusliku aluseta töötlemise ohtu. Kuidas peaks hoolitsema selle eest, et suureneva andmemahuga ei suureneks suurem oht isikuandmetele?

Rahvusvahelises õiguskirjanduses ollakse arvamusel, et tõenäoliselt vajab autode pardakaamerate kasutamine tulevikus täiendavat reguleerimist<sup>177</sup>. Kindlasti ei tohiks autori hinnangul hakata pardakaameraid seetõttu keelustama, et nad on potentsiaalseks ohuks isikuandmetele. Pigem areneb maailm selles suunas, et kaameraid tuleb juurde, näiteks USA liigub juba selles suunas, et politseinikud hakkavad kandma kehakaameraid<sup>178</sup>. Põhjus, miks politseinikud pannakse kehakaameraid kandma, on politseiniku ja tsiviilisiku suhtluse salvestamine võimalikuks hilisemaks analüüsiks ja ka politseivägivalla juhtumite vähendamiseks<sup>179</sup>. Nagu näha, on ka siin tegemist pigem praktilise väärtuse ja turvalisusega.

Rahvusvahelises õiguskirjanduses on toodud välja neli põhimõtet, kuhu pardakaameraid puudutav regulatsioon võiks liikuda sellistel juhtudel, kui tegemist ei ole isiklikuks otstarbeks salvestamisega: andmete kvaliteet ja proportsionaalsus, andmesubjekti õigused ning andmete turvalisus<sup>180</sup>.

Andmete kvaliteedi ja proportsionaalsuse all peetakse silmas, et salvestist kasutatakse eesmärgipäraselt, ehk siis kui eesmärk oli salvestada liiklusõnnetusi, siis peakski andmetöötleja

---

<sup>177</sup> Štītilis, Laurinaitis, *supra* nota 49, lk 323.

<sup>178</sup> Lawrence, M. Lights, Camera, Action: The Age of Body Cameras in Law Enforcement and the Effects of Implementing Body Camera Programs in Rural Communities. *North Dakota Law Review* 91 N.D. L. Rev. (2015), lk 611.

<sup>179</sup> *Ibid.*

<sup>180</sup> Štītilis, Laurinaitis, *supra* nota 49, lk 324.

töötlemata ainult seda lõiku, kus oli õnnetus ja loobuma muude osade töötlemisest<sup>181</sup>. See tähendab, et andmetöötleja säilitab oma kõvakettal, arvutis või ükskõik millisel andmekandjal ainult konkreetsete õnnetuste salvestusi ja muu materjali kustutab. Sama kehtiks ka avaldamise korral.

Štitilis ja Laurinaitis on veel välja pakkunud, et autod võiks tähistada teavitustega, et autos on kaamera ja toimub filmimine<sup>182</sup>. Autor puudutas sarnast mõtet ka alapunktis 1.4.1.4, kuid autori hinnangul aitaks auto pardakaamerate puhul selline teavitamisviis vältida kaamerasse jäämist ainult seisva auto puhul. Liikuva auto pardakaamera vaatevälja vältimine tundub pea võimatu.

Andmete turvalisuse all on autorid silmas pidanud nii kaamera enda kui andmekandja turvalisust, kus salvestised asuvad<sup>183</sup>. See tähendab, et auto, milles kaamerat kasutatakse, peab olema lukustatud ja andmekandjad, millel salvestised asuvad peavad olema kättesaamatud kolmandatele isikutele<sup>184</sup>. Otseselt kaamera enda turvalisust ei ole autor antud töös puudutanud ja see on kahtlemata hea mõte ka nõudeid kaamera enda turvalisusele veidi enam täpsustada. Kuna vähemalt Eestis lukustab nagunii iga hooliv autoomanik oma auto ukseid igakordsel auto juurest lahkumisel, siis autor pakub turvalisuse suurendamiseks mõtet keelata näiteks kaamera mälukaardi jätmise autosse, mis võib autosse sissemurdmise korral sattuda valede inimeste kätte. Kaamera turvalisus on oluline, kuna ka kaamera sees asub mälukaart, millel asuvad ümberkopeerimata failid ning mis valedesse kättesse sattumise korral võivad oluliselt salvestisel olevate isikute õigusi rikkuda. Andmekandjate kolmandatele isikutele kättesaamatuks tegemise mõte ei ole vähemalt Eestis midagi uut, sest vastavat teemat on puudutanud ka AKI, mida käsitles autor alapeatükis 1.3. Ka üldmääruses on sõnastatud usaldusvääruse ja konfidentsiaalsuse põhimõtte, mis tähendab, et isikuandmeid tuleb töödelda viisil, mis tagab isikuandmete asjakohase turvalisuse, sealhulgas kaitseb loata või ebaseadusliku töötlemise eest ning juhusliku kaotamise, hävitamise või kahjustumise eest, kasutades asjakohaseid tehnilisi või korralduslikke meetmeid<sup>185</sup>.

Autorile meeldib eriti Štitilise ja Laurinaitise mõtte piirata hoopis kaamera perioodi, kaua kaamera salvestisi säilitab<sup>186</sup>. Kui kaamera ainukeseks eesmärgiks on olla abivahendiks liiklusõnnetuse korral asjaolude väljaselgitamiseks, siis puudub vajadus talletada ka tundide kaupa salvestisi,

---

<sup>181</sup> *Ibid.*

<sup>182</sup> *Ibid.*

<sup>183</sup> *Ibid.*

<sup>184</sup> *Ibid.*

<sup>185</sup> OJ L 119, 04.05.2016, art 5, lg 1, p f.

<sup>186</sup> Štitilis, Laurinaitis, *supra* nota 49, lk 324.

milles on hulganisti inimeste nägusid ja muid andmeid. Piisaks, kui kaamera säilitab näiteks viimast kümnet minutit ja õnnetuse korral saab pardakaamera omanik vajalikku materjali kasutada. Töötlemise miinimumini viimise põhimõtet toetab ka üldmäärus, mis sätestab, et isikuandmed on asjakohased, olulised ja piiratud sellega, mis on vajalik nende töötlemise eesmärgi seisukohalt („võimalikult väheste andmete kogumine“)<sup>187</sup>.

Viimase mõttena pakuvad Štitilis ja Laurinaitis välja, et kindlasti peaks panustama rohkem ka auto pardakaamerate tootjad, et vähendada võimalikku isikuandmete suurenevat riivet pardakaamerate levikuga seoses<sup>188</sup>.

Autor on pigem Štitilise ja Laurinaitise pakutud ideedega nõus. Autor ei usu niivõrd kaameratega autode märgistamise efektiivsusesse, kuid kindlasti on head ideed suurendada kaamerate turvalisust. Kindlasti ei saa ja ei tohi autori hinnangul olla tulevik selline, et pardakaameraid hakatakse keelustama, sest maailm liigub pigem selles suunas, et erinevaid kaameraid tuleb juurde ja nende kõikidega tuleb maailmal kuidagi toime tulla ning koostöös kaamerate tootjate ja portaalidega tuleks suurendada andmetöötlejate teadlikkust.

Kuna sotsiaalmeedia- ja videoportaalid on paljudel juhtudel andmetöötlejatele esmaseks väljundiks, siis annaks autori hinnangul probleemiga tegeleda juba eos ehk salvestise avaldamise hetkel. Välistamiseks teadmatuses tulenevad rikkumised, saaks portaalid vaikimisi seadistusena kasutada nägude tuvastamist ja udutamist. Andmetöötlejal võiks kindlasti olla võimalus antud funktsioon ka välja lülitada, kuid seda ta saaks alles teha siis, kui on kinnitanud, et on teadlik ohtudest ja ei riku salvestise avaldamisega kellegi õigusi. Nägude tuvastamist ja udutamist võimaldab oma keskkonnas hetkel näiteks ka YouTube<sup>189</sup>, kuid tõenäoliselt ei tea enamik andmetöötlejaid sellise võimaluse olemasolust või ei oska seda kasutada.

2016. aastal jõustunud ning alates 25. maist 2018. kohalduv isikuandmete kaitse üldmäärus, mis on vahetult kohaldatav kõikides liikmesriikides, ei hakka otseselt pardakaameratega seonduvat rohkem reguleerima kui senine kehtiv õiguslik raamistik. Kaudsed mõjud ka pardakaamerate ja nende salvestiste kasutamisele üldmääruses siiski olemas.

---

<sup>187</sup> OJ L 119, 04.05.2016, art 5, lg 1, p c.

<sup>188</sup> Štitilis, Laurinaitis, *supra* nota 49, lk 324.

<sup>189</sup> YouTube. Face blurring: when footage requires anonymity, 2012. [youtube.googleblog.com/2012/07/face-blurring-when-footage-requires.html](https://youtube.googleblog.com/2012/07/face-blurring-when-footage-requires.html) (20.04.2017).

Üldmäärusega täpsustatakse isikuandmete mõistet, mis on igasugune teave tuvastatud või tuvastatava füüsilise isiku („andmesubjekti“) kohta; tuvastatav füüsiline isik on isik, keda saab otseselt või kaudselt tuvastada, eelkõige sellise identifitseerimistunnuse põhjal nagu nimi, isikukood, asukohateave, võrguidentifikaator või selle füüsilise isiku ühe või mitme füüsilise, füsioloogilise, geneetilise, vaimse, majandusliku, kultuurilise või sotsiaalse tunnuse põhjal<sup>190</sup>. Pardakaamera salvestisel oleks andmetöötlejal ilmselt kõige suurem tõenäosus avalikustada andmesubjekti asukohateave olgu siis isik salvestisel kas otseselt või kaudselt tuvastatav.

Üldmääruse üks põhimõtetest on, et isikuandmete töötlemine peab olema andmesubjektile läbipaistev<sup>191</sup>. See tähendab, et isikuandmete töötlemisega seotud teave ja sõnumid on lihtsalt kättesaadavad, arusaadavad ning selgelt ja lihtsalt sõnastatud<sup>192</sup>. Andmetöötleja jaoks tähendab see seda, et andmesubjektilt nõusoleku küsimisel või siis avalikus kohas salvestamise korral peaks andmetöötleja teavitama, kes ta on, mis on salvestamise eesmärk ning andma kogu muu vajaliku info, et tagada andmesubjektide jaoks õiglane ja läbipaistev töötlemine<sup>193</sup>. Autor toetab läbipaistvuse põhimõtet, kuid auto pardakaamerate puhul on teavitamine teatud olukordades juba niigi keeruline ja selliste detailsete andmete edastamine andmesubjektidele ei tundu reaalsena. Täpsemalt peatus autor teavitamise probleemil alapunktis 1.4.1.4. Tõenäoliselt on andmetöötlejal lihtsam kõik salvestisele jäänud isikud hägustada kui viia läbi keeruline teavitamisprotsess.

---

<sup>190</sup> OJ L 119, 04.05.2016, art 4, p 1.

<sup>191</sup> OJ L 119, 04.05.2016, art 5, lg 1, p a.

<sup>192</sup> OJ L 119, 04.05.2016, pp 39.

<sup>193</sup> *Ibid.*

## Kokkuvõte

Autorit ajendas antud teemal kirjutama sotsiaalmeedias ja uudisteportaalides pea igapäevaselt jagatavad juhtumid liikluses, mis on auto pardakaamerate vaatevälja jäänud. Üsna paljudel sellistel salvestistel on isikute näod katmata ning isikud on täielikult tuvastatavad. See tekitas autoris küsimusi ning neile vastuseid otsima asudes jõudis autor veendumusele, et Eestis on antud teemat küllaltki vähe käsitletud ning vajalik oleks inimeste teadlikkust isikuandmete ja privaatsuse osas tõsta. Meie isikuandmed vajavad üha suuremat kaitset, kuna tehnoloogia areng pidevalt suurendab võimalusi, kuidas meie isikuandmed võivad kontrollimatult ning tahtevastaselt levida. Bakalaureusetöö eesmärk oli uurida, millistel juhtudel võib füüsiline isik videomaterjali avaldada ning millistel juhtudel tuleb olla avaldamisel ettevaatlik, kuna võib avaldamisega rikkuda kellegi õigusi ning teda võidakse võtta vastutusele.

Eestis reguleerib isikuandmetega seonduvat isikuandmete kaitse seadus (IKS), mis ei kohaldu, kui andmetöötleja töötleb andmeid isiklikul otstarbel. Isiklikul otstarbel töötlemine tähendab, et salvestist ei avaldata ning salvestist säilitatakse turvaliselt, et see ei satuks kolmandate isikute valdusse. Seega isiklikul otstarbel andmete töötlemisel on välistatud ka vastutus. Kui salvestis siiski avaldada, siis on andmetöötlejal vajalik saada andmesubjekti nõusolek, mis peab põhinema tema vabal tahtel, olema konkreetne, teadlik ja ühemõtteline ning ei tohi olla tagasi võetud. Muuhulgas peab andmetöötleja arvestama, et nõusoleku olemasolu tõendamiskohustus lasub temal. Nõusolekuta on lubatud salvestis avaldada ajakirjanduslikul eesmärgil, kui esineb ülekaalukas avalik huvi, avaldamine on kooskõlas ajakirjanduseetika põhimõtetega ning ei kahjustata ülemäära andmesubjekti õigusi. Enamasti kehtivad eelpool nimetatud kolm tingimust avaliku elu tegelase puhul, kes on pidanud arvestama, et tema vastu on kõrgendatud avalikkuse tähelepanu. Kui kasvõi üks kolmest tingimusest ei ole täidetud, siis salvestise avaldamine ilma andmesubjekti nõusolekuta ei ole lubatud. Lisaks ajakirjanduslikule eesmärgile on nõusolekuta salvestise avaldamine lubatud ka asutusele, kes töötleb isikuandmeid seaduses sätestatud ülesande täitmiseks nagu näiteks politsei. Ka avalikus kohas salvestamisel eesmärgiga see hiljem avaldada tuleb saada andmetöötlejal andmesubjektidelt nõusolek. Kuna avalikus kohas võib viibida palju isikuid ja kõikidelt nõusoleku saamine võib olla mõeldamatu, siis on lubatud nõusolek asendada teavitusega sellises vormis, mis võimaldab andmesubjektil jäädvustamise faktist aru saada ning vajadusel seda vältida. Kui andmetöötlejal puudub andmesubjektide nõusolek ning ta ei ole ka andmesubjekte teavitanud, siis tuleb salvestisel kõik äratuntavad isikud hägustada. See ei puuduta

avalikku üritust, kus võib mõistlikult jäädvustamist ja selle hilisemat avaldamist eeldada. Andmesubjekti nõudmisel tuleb aga andmetöötlejal ka avalikul üritusel salvestatud materjalist andmesubjekt eemaldada või tundmatuseni hägustada.

Bakalaureusetöö leidis vastuse ka küsimusele, kuidas on võimalik isikut tuvastada. Isikut on võimalik tuvastada otseselt ja kaudselt. Otseselt on isik tuvastatav, kui isik on ilma erimeetmete ja –vahenditeta kergesti äratuntav. Seega auto pardakaamerate kontekstis on otseselt tuvastatav isik, kelle puhul on salvestisele jäänud tema nägu. Kaudse tuvastamise puhul ei ole oluline konkreetne üks näitaja, vaid pigem mitme näitaja kombinatsioon ning igas olukorras tuleb andmeid hinnata erinevalt. Seega võivad isikuandmeteks kvalifitseeruda mis tahes andmed isiku kohta olenemata nende vormist nagu näiteks eritunnustega sõiduk, millega isik sõidab või näiteks ka asukoht.

Bakalaureusetöös leidis kinnitust hüpotees, et füüsilise isiku isiklikuks otstarbeks salvestatud auto pardakaamera video avaldamine võib kaasa tuua vastutuse. Rikkumise toime pannud andmetöötleja suhtes on võimalik alustada haldus- ja tsiviilmenetlust.

Ühtlasi leidis autor vastuse bakalauresetöö uurimisküsimusele: millised on isiklikuks otstarbeks salvestatud auto pardakaamera salvestise avaldamise võimalikud tagajärjed füüsilisest isikust avaldajale. IKSis sätestatud nõuete täitmise üle teostab Eestis riiklikku ja haldusjärelvalvet AKI, kes võib algatada rikkuja suhtes haldusmenetluse. AKI roll on nõuda andmetöötlejalt avaldamise lõpetamist, teha ettekirjutusi ning määrata rikkujale korduv sunniraha, AKI ei lahenda isikutevahelisi vaidlusi, ega mõista välja kahjuhüvitisi. Maksimaalne sunniraha ülemmäär, mille AKI andmetöötlejale kehtiva seadusandluse kohaselt määrata saab, on 9600 eurot. Reeglina aga on sunniraha viimane meede ja sellele eelneb ettekirjutus. Delikaatsete isikuandmete avaldamise korral on AKI-l õigus alustada väärteomenetlust, mille tulemusena võib andmetöötleja saada trahvi kuni 300 trahviühikut, mis võrdub bakalaureusetöö kirjutamise hetkel 1200 euroga. Väärteomenetluse raames kantakse andmetöötleja ka töö kirjutamise hetkel veel avalikku karistusregistrisse, kus on võimalik andmetega tutvuda igäühel.

Andmesubjektil on oma õiguste kaitseks alati võimalus ka pöörduda tsiviilkohtusse, kus andmesubjektil on võimalik andmetöötlejalt nõuda mittevaralise kahju hüvitamist. Isikuandmete rikkumiste puhul on nimelt pea võimatu taastada rikkumisele eelnenud olukord. Mittevaralise kahju suuruse otsustab kohus võttes arvesse rikkumise raskust, ulatust ning ühtlasi ka kahju tekitaja suhtumist andmesubjekti pärast rikkumist. Lisaks on andmesubjektil õigus olulise õiguste

riive korral nõuda moraalse kahju hüvitamist valuraha kujul. Valuraha saab nõuda vaid juhul, kui kahju ei ole võimalik muul viisil heastada ja autori hinnangul võiks moraalse kahju hüvitamine tulla kõne alla juhul, kui salvestis saab erakordselt suure tähelepanu osaliseks ja andmesubjekt on sellel salvestisel selgelt äratuntav. Ka moraalse kahju hüvitamise korral otsustab kohus võttes arvesse õiguse üldpõhimõtteid (sh võrdsus), ühiskonna üldise heaolu taseme, kohtupraktika, rikutud õiguse kaalukuse ja „valu suuruse”.

Bakalaureusetöö panustab õigusteadliku uurimise edendamisse teema analüüsimisega auto pardakaamerate vaatenurgast, kuna auto pardakaamerate populaarsus on kasvavas trendis ja salvestiste avaldamise aspektist tuleb teha üha enam teavitustööd.

Bakalaureusetöö pakub uudseid lahendusi, kuidas leevendada isikuandmete avaldamisega seotud rikkumisi. Autori hinnangul tuleks antud valdkonda tulevikus rohkem reguleerida selliselt, et salvestisi kasutataks eesmärgipäraselt. See tähendab, et kui eesmärk on salvestada näiteks liiklusõnnetusi, siis andmetöötleva töötlebki ainult seda kindlat õnnetuse lõiku ja muu kustutab. Kindlasti tuleks välja töötada turvanõuded, kuidas kaamerat ja seal sees asuvat mälukaarti tuleb igapäevaselt käsitleda. Näiteks üks nõudmine võiks olla, et kaamerat või selle mälukaarti ei tohi jätta autosse isegi, kui see on lukustatud. Kindlasti pakuks isikuandmetel rohkem turvalisust, kui piirata kaamera salvestiste säilitamise aega näiteks kümnele minutile. See jätkaks endiselt autoomanikule võimaluse kasutada pardakaamerat eesmärgipäraselt, ehk salvestada liiklusõnnetus ja pakuks piisavat kaitset isikuandmetele, mis salvestisele jäävad. Uudne lahendus oleks kindlasti, kui sotsiaalmeedia- ja videoportaalid hakkaksid tulevikus pakkuma salvestise üleslaadimisel vaikimisi nägude hägustamist. Kasutajale säiliks võimalus antud funktsioon lihtsa nupuvajutusega välja lülitada, kuid see oleks hea koht, kus andmetöötlevale meelde tuletada, et kas ta on ikka kindel, et salvestise avaldamisega ei avalda ta tahtmatult kellegi isikuandmeid.

# **Legal Regulation of the Publication of Personal Data in the Context of Publishing Data on the Example of Car Onboard Cameras**

## **Abstract**

Our personal data are increasingly in need of protection, as developments in technology are constantly increasing the risk that our personal data can become public against our will and without a way for us to control it. The aim of the Bachelor's thesis is to look at the cases when a natural person is entitled to publish video material and the cases when one should be careful with the publication, as this may infringe on somebody's rights and can result in legal charges.

Issues related to personal data are regulated in Estonia with the Personal Data Protection Act (PDPA), which does not apply if data are processed for personal needs. Processing data for personal needs means that a recording will not be published and will be kept securely, so that it cannot fall into the hands of third persons. Thus, if data is processed for personal purposes, legal responsibility is excluded. Should one still want to publish a recording, the processor of the data will have to obtain consent from the data subject, and the consent must be based on the subject's free will, be specific, intended and unequivocal, and it must not be revoked. The data processor will have to consider, among other things, that it is up to the processor to prove the existence of consent. It is allowed to publish recordings without consent for journalistic purposes if there is considerable public interest, the publication complies with the principles of journalist ethics and does not damage the rights of the data subject excessively. Should one of the three conditions not be fulfilled, publication of the recording without the data subject's consent is prohibited. In addition to the journalistic purposes, recordings can also be made accessible to institutions that process personal data for fulfilling purposes stipulated by law, like the police. When recording in a public place with the aim of later publishing the recording, the data processor has to obtain the consent of the data subject. As the number of people potentially present at a public location can be large and obtaining consent from all of them can be unthinkable, it is permitted to replace the consent with a notice in a form that permits the data subjects to understand the fact of the recording and to avoid it if they so wish. If the data processor does not have the consent of the data subjects and he or she has not notified the data subjects, all recognisable persons in the recording must be blurred. This does not concern public events, where reasonable recording and later publication of the recording can be presumed. However, should the data subject require this, he or she must also

be removed or blurred to the point of making them unrecognisable even in the case of recordings made at a public event.

The hypothesis that publication of a video recorded by a natural person for personal purposes using a car onboard camera can result in legal accountability is corroborated in the thesis. Administrative or civil proceedings can be started against a data processor who has committed a violation.

The author also finds an answer to the study question of the thesis: what are the possible consequences that publishing a recording made for personal purposes with a car onboard camera can bring to a natural person. Compliance with the requirements of the PDPA is monitored in Estonia by the Data Protection Inspectorate (DPI) that can start administrative proceedings against violators. It is the role of DPI to request that the data processor desist from publishing the recording, to issue precepts and to penalize a violator with a repeated penalty payment; DPI does not solve disputes between persons nor decree payments of compensation for damages. The maximum amount that DPI can penalize a data processor with according to the presently valid legislation is 9,600 euros. As a rule, however, penalty payments is the last resort, preceded by a precept. If delicate personal data have been published, DPI has the right to initiate a misdemeanour proceeding, which may result in a fine of up to 300 fining units for the data processor, which equals 1,200 euros at the time of the writing of the thesis. A part of the misdemeanour proceeding is also the recording of the data of the data processor in the Criminal Record Registry, still public at the time of the writing and accessible to everyone.

The data subject also has the right to apply to a civil court, where the data subject can request compensations for non-material damages from the data processor. This is because in the case of a violation involving personal data it is almost impossible to restore the situation as it was before the violation. The volume of the non-material damages will be decided by the court, considering the gravity and extent of the violation as well as the attitude of the person causing the damages towards the data subject after the violation. The data subject is also entitled to request compensation for moral damages in the form of reparation if his or her rights have been violated significantly. Reparation can be demanded only if there is no other way to repair the damage and the author finds that compensation for moral damages can be discussed if the recording is met with remarkable attention when published and if the data subject is clearly recognisable in the recording. In the case of compensation of moral damages, the court will also consider the general

principles of law (including equality), the general level of welfare in the society, previous court practice, the weight of the violated right and the 'amount of pain'.

The thesis contributes to furthering legal research by analysing the topic from the point of view of the car onboard camera, as the use of such cameras is increasing and there is a need to raise awareness about the topics surrounding the publication of these recordings.

The thesis proposes innovative solutions about how to mitigate violations related to the publication of personal data. The author finds that this area needs more regulation in the future so that the recordings were used for their intended purpose. This means that if, for instance, the aim is to record traffic accidents, the data processor will process only the part of the recording where an accident occurs, and deletes everything else. There is a definite need to develop security measures on how the camera and its memory card should be handled in an everyday situation. One of the requirements could be, for example, that the camera or its memory card should not be left in the car, even if it is locked. Personal data would definitely be better protected if the storage time of the recording was limited, for example to 10 minutes. This would give the car owner the opportunity to keep using the onboard camera for its intended purpose, i.e. to record traffic accidents, and would provide sufficient protection to the personal data recorded. It would be an innovative solution for social media and video portals to start blurring faces by default in uploaded recordings. Users would have the option to switch this feature off with a click, but it would be a great way to remind the data processor that he or she has to make sure that nobody's personal data is unwillingly violated with the publication of the recording.

## Kasutatud allikate loetelu

### Teadusraamatud:

1. Männiko, M. Õigus privaatsusele ja andmekaitse. Tallinn, Juura 2011.
2. Tikk, E., Nõmper, A. Informatsioon ja õigus. Tallinn, Juura 2007.

### Teadusartiklid:

3. Aleksejeva, P. Isikust tehtud kujutise avaldamise õiguspärasus, magistritöö, Tartu Ülikooli Õigusteaduskond 2013.
4. Buitelaor, J.C. Privacy: Back to the Roots. *German Law Journal* 13 German L.J. (2012).
5. De Filippi, P., Belli, L. Law of the Cloud v Law of the Land: Challenges and Opportunities for Innovation. *European Journal of Law and Technology*, Vol 3, Issue 2, 2012.
6. De Hert, P., Papakonstantinou, V. The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals. *Computer law & security review* 28 (2012).
7. DeVries, W.T. Protecting Privacy in the Digital Age, *Berkeley Technology Law Journal* 18 Berkeley Tech. L.J. (2003).
8. Gundermann, L. Euroopa Liidu andmekaitseõigus – andmekaitse ja andmetele avaliku juurdepääsu suhtest ning andmekaitse järelevalve olukorrast. *Juridica VIII/2005*.
9. Ikkonen, K. Avalik huvi kui määratlemata õigusmõiste. *Juridica III/2005*.
10. Ilus, T. Isikuandmete kaitse olemus ja arengusuunad. *Juridica VII/2002*.
11. Kotschy, W. The proposal for a new General Data Protection Regulation—problems solved? *International Data Privacy Law*, 2014, Vol. 4, No. 4.
12. Kuner, C. The European Union and the Search for an International Data Protection Framework. *Groningen Journal of International Law*, vol. 2, ed. 1: Privacy in International Law.
13. Kungas, M. Traditsiooniliste õiguskaitsevahendite rakendatavus isikuandmete kaitse õiguse tagamisel infoühiskonnas ja nende võimalikest arengutest, magistritöö, Tartu Ülikooli Õigusteaduskond 2015.
14. Lawrence, M. Lights, Camera, Action: The Age of Body Cameras in Law Enforcement and the Effects of Implementing Body Camera Programs in Rural Communities. *North Dakota Law Review* 91 N.D. L. Rev. (2015).

15. Pilving, I. Sugupuud müügiks ja roolijoodikud häbiposti? Isikuandmetega seonduvad piirangud avaliku teabe avaldamisel. *Juridica* II/2004.
16. Pilving, I. Õigus isikuandmete kaitsele. *Juridica* VIII/2005.
17. Rengel, A. Privacy-Invasive Technologies and Recommendations for Designing a Better Future for Privacy Rights. *Intercultural Human Rights Law Review*, 2013, Vol. 8.
18. Robinson, N., Graux, H., Botterman, M., Valeri, L. Review of the European Data Protection Directive. Cambridge, Rand Europe 2009.
19. Rustad, M.L., Kulevska, S, Reconceptualizing the Right To Be Forgotten To Enable Transatlantic Data Flow. *Harvard Journal of Law & Technology*, 2015, vol 28.
20. Sillaots, S. Isikuandmete kaitse regulatsiooni ühtlustamine isikuandmete kaitse üldmääruse eelnõus ja selle mõju Eestile, magistritöö, Tartu Ülikooli Õigusteaduskond 2014.
21. Sootak, J. Karistusõiguse revisjon kuriteo-, väärteo- ja haldusõiguse piirimal. *Juridica* IV/2013.
22. Štītilis, D., Laurinaitis, M. Legal regulation of the use of dashboard cameras: Aspects of privacy protection. *Computer law & security review* 32 (2016).
23. Tammer, S. Kujutis kui tegelikult kaitstav õigushüve. *Juridica* IX/2011.
24. Tampuu, T. Deliktiõigus võlaõigusseaduses. Üldprobleemid ja delikti üldkoosseisul põhinev vastutus. *Juridica* II/2003.
25. Tupay, P. T. Õigusest eraelule kuni andmekaitse üldmääruseni ehk tundmatu õigus isikuandmete kaitsele. *Juridica* IV/2016.

Eesti õigusaktid:

26. Eesti Vabariigi põhiseadus RT I, 15.05.2015, 2.
27. Haldusmenetluse seadus RT I, 25.10.2016, 5.
28. Isikuandmete kaitse seadus RT I, 06.01.2016, 10.
29. Karistusregistri seadus RT I, 30.12.2015, 17.
30. Karistusseadustik RT I, 31.12.2016, 14.
31. Korrakaitse seadus RT I, 02.12.2016, 6.
32. Tsiviilseadustiku üldosa seadus RT I, 12.03.2015, 106.
33. Võlaõigusseadus RT I, 11.03.2016, 2.

EL-i ja rahvusvahelised õigusaktid:

34. OJ C 83, 30.3.2010.
35. OJ L 119, 04.05.2016.
36. OJ L 281, 23.11.1995.

Eesti kohtulahendid:

37. RKHKo 3-3-1-3-12, p 19.
38. RKÜKo 3-2-1-4-13, p 17.
39. RKHKo 3-3-1-85-15, p 4.
40. RKTKo 3-2-1-152-09, p 14.
41. RKTKo 3-2-1-159-14, p 13.
42. RKÜKo 3-2-1-4-13, p 17.

Muud kohtulahendid:

43. EIKo 26.11.1991, 13585/88, *Observer and Guardian v. The United Kingdom*
44. EKo 09.11.2010, C-92/09 ja C-93/09, *Volker und Markus Schecke, Hartmut Eifert*
45. EKo 24.11.2011, C- 468/10 ja C-469/10, *ASNEF ja FECEMD*
46. Eko 13.05.2014, C-131/12, *Google Spain SL, Google Inc. v. Agencia de Protección de Datos (AEPD), Mario Costeja González*
47. EKo 11.12.2014, C-212/13, *Ryneš*
48. EKo 19.10.2016, C-582/14, *Breyer vs Saksamaa Liitvabariik*

Muud allikad:

49. § 19, p 3.1.2.1. Põhiõigused ja Vabadused. II peatükk. Eesti Vabariigi põhiseadus. Kommenteeritud väljaanne. [www.pohiseadus.ee/ptk-2/](http://www.pohiseadus.ee/ptk-2/) (09.12.2016).
50. § 25, p 2.4.2. Põhiõigused, vabadused ja kohustused. II peatükk. Eesti Vabariigi põhiseadus. Kommenteeritud väljaanne. [www.pohiseadus.ee/ptk-2/pg-25/](http://www.pohiseadus.ee/ptk-2/pg-25/) (05.03.2017).
51. Andmekaitse Inspektsioon. Isikuandmete avalikustamine meedias: Andmekaitse Inspektsiooni sekkumiskriteeriumid, 2015. [www.aki.ee/sites/www.aki.ee/files/elfinder/article\\_files/Juhised/meediavaidlusse%20sekumise%20kriteeriumid.pdf](http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/Juhised/meediavaidlusse%20sekumise%20kriteeriumid.pdf) (05.03.2017).
52. Andmekaitse Inspektsioon. Andmekaitse Inspektsiooni peadirektori ülevaade andmekaitsereformi rakendamise seisust Eestis 14.10.2016, 2016.

- [www.aki.ee/sites/www.aki.ee/files/elfinder/article\\_files/ylevaade\\_reformist\\_14102016.pdf](http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/ylevaade_reformist_14102016.pdf) (09.04.2017).
53. Andmekaitse Inspeksioon. Avaliku teabe seaduse ja isikuandmete kaitse seaduse täitmisest aastal 2015. Soovitused aastaks 2016, 2016. [www.aki.ee/sites/www.aki.ee/files/elfinder/article\\_files/AASTARAAMAT.pdf](http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/AASTARAAMAT.pdf) (05.03.2017).
54. Andmekaitse Inspeksioon. Juhend kaamerate kasutamise kohta, 2016. [www.aki.ee/sites/www.aki.ee/files/elfinder/article\\_files/kaamerate%20juhis%20\(01.07.2016\).pdf](http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/kaamerate%20juhis%20(01.07.2016).pdf) (21.11.2016).
55. Andmekaitse Inspeksioon. Avaliku teabe seaduse ja isikuandmete kaitse seaduse täitmisest 2016. aastal. Soovitused aastaks 2017, 2017. [www.aki.ee/sites/www.aki.ee/files/elfinder/article\\_files/aastaraamat\\_2016.pdf](http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/aastaraamat_2016.pdf) (22.04.2017).
56. Article 29 Data Protection Working Party. Opinion 4/2007 on the concept of personal data, 2007. [www.clinicalstudydatarequest.com/Documents/Privacy-European-guidance.pdf](http://www.clinicalstudydatarequest.com/Documents/Privacy-European-guidance.pdf) (24.04.2017).
57. Credence Research, The Global Dashcams Market to Reach US\$ 5,530.0 Mn by 2022, 2016. [www.credenceresearch.com/press/the-global-dashcams-market](http://www.credenceresearch.com/press/the-global-dashcams-market) (03.04.2017).
58. Delfi.ee. VIDEO: Liiklusraev ja võõraviha Tallinnas: ohtliku olukorra tekitanud mees peatas keset teed auto ja ähvardas järeleõitjat kurikaga. [www.delfi.ee/news/paevauudised/krimi/video-liiklusraev-ja-vooraviha-tallinnas-ohtliku-olukorra-tekitanud-mees-peatas-keset-teed-auto-ja-ahvardas-jarelsoitjat-kurikaga?id=74476625](http://www.delfi.ee/news/paevauudised/krimi/video-liiklusraev-ja-vooraviha-tallinnas-ohtliku-olukorra-tekitanud-mees-peatas-keset-teed-auto-ja-ahvardas-jarelsoitjat-kurikaga?id=74476625) (27.04.2017)
59. Eesti Ajalehtede Liit. Eesti ajakirjanduseetika koodeks. [www.eall.ee/eetikakoodeks.html](http://www.eall.ee/eetikakoodeks.html) (14.01.2017).
60. Eesti Maksumaksjate Liit. Riigikogu liikmetele makstud kuluhüvitised sõiduautode rendi ja liisingu eest, 2015. [www.maksumaksjad.ee/modules/news/article.php?storyid=8354](http://www.maksumaksjad.ee/modules/news/article.php?storyid=8354) (28.01.2017).
61. Euroopa Liidu Teataja, L 119, 4. mai 2016
62. Isikuandmete kaitse seaduse eelnõu seletuskiri. [www.aki.ee/sites/www.aki.ee/files/elfinder/article\\_files/IKS%20SELETUSKIRI%20%281%29.rtf](http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/IKS%20SELETUSKIRI%20%281%29.rtf) (14.01.2017), § 11.

63. Justiitsministeerium. Justiitsministeeriumi ja haldusala struktuur. [www.just.ee/et/ministeerium-kontaktid/ministeeriumi-tutvustus-ja-struktuur](http://www.just.ee/et/ministeerium-kontaktid/ministeeriumi-tutvustus-ja-struktuur) (05.03.2017).
64. Komisjoni teatis euroopa parlamendile, nõukogule, majandus- ja sotsiaalkomiteele ning regioonide komiteele. Terviklik lähenemisviis isikuandmete kaitsele Euroopa Liidus, 2010. [ec.europa.eu/justice/news/consulting\\_public/0006/com\\_2010\\_609\\_et.pdf](http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_et.pdf) (04.03.2017).
65. Postimees: AKI hajutab lugejate kahtlusi, 2015. [www.aki.ee/et/uudised/meediakajastus/postimees-aki-hajutab-lugejate-kahtlusi](http://www.aki.ee/et/uudised/meediakajastus/postimees-aki-hajutab-lugejate-kahtlusi) (14.01.2017).
66. Postimees. Autokaamerad aitavad kindlustusel lahendada mitmeid juhtumeid kuus, 2016. [tarbija24.postimees.ee/3960039/autokaamerad-aitavad-kindlustusel-lahendada-mitmeid-juhtumeid-kuus](http://tarbija24.postimees.ee/3960039/autokaamerad-aitavad-kindlustusel-lahendada-mitmeid-juhtumeid-kuus) (28.04.2017).
67. Postimees. Video: Juhan Parts lõhkus bensiinjaamas tankuri, 2016. [tallinncity.postimees.ee/3853807/video-juhan-parts-lohkus-bensiinjaamas-tankuri](http://tallinncity.postimees.ee/3853807/video-juhan-parts-lohkus-bensiinjaamas-tankuri) (28.01.2017).
68. YouTube. Face blurring: when footage requires anonymity, 2012. [youtube.googleblog.com/2012/07/face-blurring-when-footage-requires.html](http://youtube.googleblog.com/2012/07/face-blurring-when-footage-requires.html) (20.04.2017).