PRIVAATSUSÕIGUS INIMÕIGUSENA JA IGAPÄEVATEHNOLOOGIAD

Privaatõiguse ja andmekaitse õiguslikud aspektid

Katrin Nyman Metcalf

SISUKORD

SISUKORD 81

SISSEJUHATUS 82

PRIVAATSUSÕIGUSE KUJUNEMINE: AJALOOLINE TAUST 83

OLULISEMAD ÕIGUSLIKUD PÕHIMÕTTED ISIKUANDMETE KAITSMISEL 84

PRIVAATSUSÕIGUS INIMÕIGUSENA 85

PRIVAATSUSÕIGUS JA ISIKUANDMETE KAITSE EUROOPA LIIDU JA EESTI ÕIGUSES 88

EUROOPA LIIDU ANDMEKAITSEALANE ÕIGUS 88
EESTI ANDMEKAITSE ÕIGUSSÜSTEEM 90
EESTI PÕHISEADUS 90
ISIKUANDMETE KAITSE SEADUS JA MUUD ÕIGUSAKTID 90
JÄRELEVALVE 92

LÕPETUSEKS VÄLJAKUTSETEST ANDMEKAITSEÕIGUSELE 93

SISSEJUHATUS

Ühiskonnas, kus inimesed elavad koos, ei ole täielik privaatsus võimalik. Moodne informatsiooni- ja kommunikatsioonitehnoloogia (IKT) on võimaldanud uusi viise, kuidas suhelda, jagada ja koguda infot, käia läbi sõpradega või kohata uusi inimesi, anda nõu, valitseda riiki ja palju muud. Meil on võimalik suhelda peaaegu terve maailmaga vahetult – viisil, mis ainult mõned aastakümned tagasi oli mõeldamatu. Eeliseid on väga palju, aga uute suhtlusviisidega kaasnevad ka riskid. Kui terve maailm muutub külaks, kus kõik teavad teistest kõiki, mis siis juhtub privaatsusega? Isikute suhtumine ja hoiakud on selles kontekstis olulised, aga peab aru saama ka õiguslikku konteksti, mis loob hoiakutele raami.

Õiguslikust aspektist on andmekaitse osa privaatsusõigusest, mis on kaitstud kui inimõigus nii riikide põhiseaduste kui ka rahvusvaheliste konventsioonide kaudu[1]. See tähendab, et andmekaitse põhimõtted olid olemas juba enne, kui sellest andmekaitse nime all konkreetselt räägiti ja sellenimelisi seadusi vastu võeti. Tänapäeval on see seos jätkuvalt oluline. Ka nendes riikides, kus puudub andmekaitseseadus, on tavaliselt olemas õigus teatudandmekaitsele, kuna peaaegu kõik maailma riigid on liitunud mõne inimõiguste lepinguga. Eestis on nii põhiseaduses kui ka muus seadusandluses mitmeid privaatsust ja andmeid kaitsvaid sätteid. Lisaks on asutatud andmekaitse sõltumatu järelevalveasutus Andmekaitse Inspektsioon.

Andmekaitse kui eraldi teema nii õigusteaduse aruteludes kui ka seadusandluses sai alguse 1970. ja 1980. aastatel – ajal, mil andmete automaatne töötlemine muutus tavapäraseks. Tehnoloogilise arenguga on andmed muutunud väga väärtuslikuks ja oluliseks: suuri andmehulki saab kasutada eri teenuste pakkumiseks, mis enne automaatset töötlemist ei oleks olnud võimalik. Andmevahetus ja ristkasutus on eri andmetel põhinevate avalike ja erateenuste jaoks olulised. Siiski peaks andmekaitse olemus olema seotud andmete sisu ja mitte nende vormiga. Põhimõtteliselt ega õiguslikult ei ole oluline, kas andmeid säilitakse ja töödeldakse elektrooniliselt või muul viisil. Praktiliselt võib see tähendada olulisi erinevusi, millega õigussüsteem peab arvestama, tagades, et reeglid sobivad eri olukordades. Andmekaitse suhtes peab otsustama, kas ja kuidas saab elektroonilises maailmas kaitsta andmeid sama hästi kui nn pärismaailmas. Ei ole ebatavaline, et püüdes luua turvalist *on-line* ühiskonda luuakse rohkem piiranguid, kui nö *off-line* keskkonnas. Tehnoloogiad võivad pakkuda ka uusi võimalusi andmekaitse paremaks tagamiseks. Tänu moodsatele tehnoloogiatele on andmete töötlemine muutunud turvalisemaks, need ei tekita vaid uusi riske. Näiteks jätavad toimingud andmebaasis „jalajälje", st kui keegi vaatab andmeid, on logidest võimalik kontrollida, kas, millal ja kes seda tegi. See raskendab oluliselt näiteks ametnike poolset andmete kuritarvitamist või hooletust ja aitab suurendada inimeste usaldust elektrooniliste andmebaaside vastu.

Mitmed meedias kajastatud skandaalid telefonikõnede pealtkuulamisest või e-mailide lugemisest on tekitanud arutelu privaatsuse tähenduse ja olulisuse kohta. Samas käituvad

[1] Isikuandmete kaitse seaduse §-s 1 on sätestatud järgmine: „Seaduse eesmärk on kaitsta isikuandmete töötlemisel füüsilise isiku põhiõigusi ja -vabadusi, eelkõige õigust eraelu puutumatusele".

inimesed jätkuvalt nii, et tegelikult on nende kohta väga palju andmeid enam-vähem avalikult kättesaadavad nende enda tegevuse tõttu, nt Facebooki kasutamise või lihtsalt mobiiltelefoni kaasas kandmise tõttu, mille kaudu saab kontrollida, kus keegi viibib. Andmekaitse seisukohast peab kaaluma, missugused andmed on sellised, et peaks takistama nende üldist kättesaadavust. Teatud andmed – ükskõik mis vormis – võivad aga olla üldiselt nähtavad või muidu kättesaadavad. Kuna inimeste teadlikkus selle kohta, kas ja kuidas saab andmeid kaitsta, ei ole tihti eriti suur, on oluline, et õigussüsteem pakub tuge paralleelselt teadmiste parandamisega.

PRIVAATSUSÕIGUSE KUJUNEMINE: AJALOOLINE TAUST

Andmekaitse ei ole iseenesest seotud moodsa tehnoloogiaga, aga samas on selle tähtsus kindlasti tehnoloogia tõttu kasvanud. Maailma esimene andmekaitseseadus võeti vastu Saksa liidumaal Hessenis 1970. aastal. Rootsi oli esimene riik, kus riigi tasandil võeti vastu andmekaitseseadus 1973. aastal, sellele järgnesid peagi mitmed seadused eri riikides[2]. Esimene oluline rahvusvaheline dokument, milles sõnastati andmekaitse põhiprintsiibid, nt eesmärgipärasus ja proportsionaalsus, oli OECD 1980. aasta deklaratsioon isikuandmete kaitse ja piiriülese liikumise juhtnööridega[3]. Juba 1983. aasta detsembris võttis Saksa Liitvabariigi konstitutsioonikohus vastu otsuse, mille kohaselt peeti rahvaloenduse teatud aspekte põhiõigustega vastuolus olevaks üksikisiku eraelu puutumatuse tõttu[4]. See kõik juhtus ajal, kui hakati kasutama aina rohkem arvutipõhist andmetöötlemist. Tehnika tõi esile andmekaitse olulisuse, kuna nüüd oli võimalik väga suurel hulgal andmeid töödelda, et neist mingit kasulikku teavet kätte saada. Tehnoloogia abil võib suurest hulgast üksikasjalikest andmetest midagi aru saada – kombineerida erinevaid andmeid nii, et iseenesest vähetähtsad andmed muutuvad oluliseks, ning koguda ja levitada andmeid üle kogu maailma. Kindlasti on tehnoloogia loonud uue keskkonna, milles tuleb andmekaitset rakendada[5].

OECD deklaratsioonis ning ka Euroopa Liidu (EL) õigusaktides on andmekaitse taustaks andmete töötlemine ja eriti andemete liikumine riikide vahel. 1970. ja 1980. aastatel oli selline andmete liikumine tööd- ja aega nõudev protsess, millele sai rakendada erinevaid reegleid. Automaatse andmevahetuse tehnilised võimalused olid oluline põhjus andmevahetuse reeglite loomiseks, kuna enam ei olnud võimalik iga juhtumi puhul üksikasjalikult uurida, mis viisil peaks andmeid teistele riikidele ja/või asutustele edastama.

---

[2] Fraunhofer Fokus (P. Hoepner, L. Strick, M. Löhe) *Historical Analysis on European Data Protection Legislation.* Report, March 2012, lk 11–12. www.fokus.fraunhofer.de.

[3] *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.* http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm. Dokumenti on 2013. aastal muudetud.

[4] Fraunhofer Fokus (P. Hoepner, L. Strick, M. Löhe) *Historical Analysis on European Data Protection Legislation.* Report, March 2012, lk 12. www.fokus.fraunhofer.de.

[5] G. Gonzales Fuster, S. Gutwirth, P. de Hert (2010) „From Unsolicited Communications to Unsolicited Adjustments": G. Gutwirth,Y. Poullet & P. de Hert (toim.) *Data Protection in a Profiled World*, Springer, Dordrecht/London (105-117), lk 107–109.

IKT kiire arenguga viimase paarikümne aasta jooksul on kaasnenud uus olukord, kus eraettevõtetel on suurel hulgal andmeid isikute kohta, mida nad on saanud isikute endi käest kas otseselt selle kaudu, et inimesed on neid andmeid internetti (näiteks Facebooki) ise üles pannud, või selle kaudu, et inimesed on kasutanud internetiteenust (näiteks Google), mille kaudu nende kohta saab erinevaid asju teada. Mitmetel firmadel, kaasa arvatud nimetatud suurtel rahvusvahelistel ettevõtetel Facebook ja Google, on eetilised reeglid ja nende rakendamiseks loodud eri struktuurid. Need on aga ettevõtte eneseregulatsiooni kaudu loodud reeglid, mis põhinevad peamiselt heal tahtel. Lisaks kehtib riikide seadusandlus vaatamata sellele, et tegemist on rahvusvaheliste ettevõtetega, millel võib puududa teatud jurisdiktsiooniga otsene seos. Tegelikult võib aga olla keeruline rakendada seaduseid eelkõige jurisdiktsiooniga seotud põhjustel.

OLULISEMAD ÕIGUSLIKUD PÕHIMÕTTED ISIKUANDMETE KAITSMISEL

Andmekaitset käsitlev õiguslik regulatsioon ja selle rakendamise süsteem on muutunud vähe alates selle õigusvaldkonna sünnist. Põhjus, miks andmeid on vaja kaitsta, on see, et nende sisu mõjutab isikute eraelu, mis peaks olema puutumatu ja mille üle isikud peaksid ise otsustama. Andmekaitse spetsiifilised reeglid sisaldavad näiteks õigust saada juurdepääsu andmetele ning parandada teavet enda kohta. Oluline on, et isik teab, mis andmeid on tema kohta olemas ja ta saab kontrollida, et need on korrektsed. Tähtis osa andmekaitsest on järelevalve, kuid samas ei ole võimalik sätestada iga olukorra kohta, mis andmeid ja kuidas tohib jagada – selleks on olukorrad liiga erinevad. Oluline on, et on loodud sõltumatu amet, kes vastutab andmekaitse järelevalve eest ja kelle pädevusse kuulub ka soovituste ja juhiste andmine erinevate olukordade kohta. Asutuste puhul on tähtis, et neis töötavad pädevad isikud, kes vastutavad andmete eest. Jätkuvalt juhtub, et asutuste või ettevõtete IT-osakonnad vastutavad igasuguste elektrooniliste andmete eest, kaasa arvatud küsimuste eest, mis on pigem andmete sisu kui vormiga seotud ja millega peaksid tegelema teistsuguse pädevusega isikud.

Isiku nõusolek on andmekaitse puhul oluline. Tihti on andmete kogumiseks ja töötlemiseks vaja nõusolekut, kuigi on ka mitmeid olukordi, kus riigid (aga tavaliselt mitte eraettevõtted) tohivad teatud andmeid koguda ka nõusolekuta. Nõusolek peab olema teadlik, see tähendab, et isikul on piisavalt teavet, et saada aru, millele ta nõusoleku annab, ning ta teeb seda vabatahtlikult. Isik võib oma nõusoleku ka igal ajal tagasi võtta.

Andmed, mida kaitstakse, on isikuandmed, mis sisaldavad mis tahes teavet tuvastatud või tuvastatava füüsilise isiku kohta, arvestades, et tuvastatav isik on isik, keda saab otseselt või kaudselt tuvastada, eelkõige isikukoodi põhjal või ühe või mitme tema füüsilisele, füsioloogilisele, vaimsele, majanduslikule, kultuurilisele või sotsiaalsele identsusele omase joone põhjal[6]. Andmed võivad olla rohkem või vähem delikaatsed, aga kõik andmed tuvastatud isikute kohta on seaduse mõistes isikuandmed ja neid tuleb töödelda ettenähtud korras. Andmekaitse seaduste eesmärk on eelkõige tagada kord andmete töötlemiseks –

mitte seda takistada. Andmed on olulised ühiskonnale, aga neid tuleb käsitleda nii, et tagataks nende korrektsus ja välditaks mitte-eesmärgipärast või isegi kahjustavat kasutust.

Enamiku riikide andmekaitseseaduses on eraldi ära toodud, mida peetakse silmas delikaatsete isikuandmetega. ELi direktiivis 95/46/EÜ nimetatakse eraldi selliseid isikuandmeid, mis paljastavad rassilise või etnilise päritolu, poliitilised vaated, usulised või filosoofilised veendumused, ametiühingusse kuulumise, tervislikku seisundit või seksuaalelu[7]. Täpse definitsiooni delikaatsete isikuandmete kohta kehtestab iga riik ise nii seadusandluses kui ka kohtupraktika kaudu ja sellest tulenevalt on näha kultuurist ja ajaloost tingitud riikidevahelisi erinevusi[8].

PRIVAATSUSÕIGUS INIMÕIGUSENA

ÜRO 1948. aasta inimõiguste ülddeklaratsioon[9] ning 1950. aasta Euroopa inimõiguste ja põhivabaduste kaitse konventsioon (EIÕK)[10] hõlmavad privaatsusõigust või eraelu puutumatust, mis on jätkuvalt aluseks andmekaitsele. Ka regionaalsed inimõiguste konventsioonid väljaspool Euroopat sisaldavad sarnaseid õiguseid. Esimene oluline inimõiguste dokument, kus nimetatakse otseselt andmekaitset, on ELi põhiõiguste harta, mis kuulutati välja 2000. aastal ja tehti õiguslikult siduvaks ning osaks ELi aluslepingutest 2009. aastal jõustunud Lissaboni lepinguga. Põhiõiguste hartas on andmekaitse eraldi välja toodud artiklis 8, kuna aga üldine privaatsuse kaitse on ka olemas, artiklis 7. Varem on andmekaitset toetatud ainult privaatsusõiguse artiklite kaudu. ELi põhiõiguste harta artikkel 8 annab õiguse saada juurdepääs ning ka parandada andmeid enda kohta. Lisaks sätestab see artikkel, et peab olema loodud sõltumatu amet, mis tegeleb andmekaitse järelevalvega (nagu see on sätestatud ELi direktiivis andmekaitse kohta)[11].

---

[6] Direktiivi 95/46/EÜ artikkel 2. Mitmed andmekaitseseadused, eelkõige ELis aga ka mujal, kasutavad väga sarnast terminoloogiat.

[7] Direktiivi 95/46/EÜ artikkel 8.

[8] Vastav säte Eesti isikuandmete kaitse seaduses:

§ 4. Isikuandmed

(1) Isikuandmed on mis tahes andmed tuvastatud või tuvastatava füüsilise isiku kohta, sõltumata sellest, millisel kujul või millises vormis need andmed on.

(2) Delikaatsed isikuandmed on:

1) poliitilisi vaateid, usulisi ja maailmavaatelisi veendumusi kirjeldavad andmed, välja arvatud andmed seadusega ettenähtud korras registreeritud eraõiguslike juriidiliste isikute liikmeks olemise kohta;

2) etnilist päritolu ja rassilist kuuluvust kirjeldavad andmed;

3) andmed terviseseisundi või puude kohta;

4) andmed pärilikkuse informatsiooni kohta;

5) biomeetrilised andmed (eelkõige sõrmejälje-, peopesajälje- ja silmaiirisekujutis ning geeniandmed);

6) andmed seksuaalelu kohta;

7) andmed ametiühingu liikmelisuse kohta;

8) andmed süüteo toimepanemise või selle ohvriks langemise kohta enne avalikku kohtuistungit või õigusrikkumise asjas otsuse langetamist või asja menetluse lõpetamist.

[9] http://vm.ee/et/uro-inimoiguste-ulddeklaratsioon.

[10] https://www.riigiteataja.ee/akt/78154.

[11] K. Nyman-Metcalf (2014:2) „The Future of Universality of Rights": T. Kerikmäe (toim.) *Protecting Human Rights in the EU*, Springer, Heidelberg (21-35): lk 28–30.

Erinevalt ELi põhiõiguste hartast ei ole maailma tasemel konventsioonides või sarnastes dokumentides andmekaitset eraldi välja toodud. Privaatsusõigus on aga olemas ja selle alusel ka teatud andmekaitse. Mitmes maailma riigis puudub andmekaitseseadus ja kuigi nendes riikides saab privaatsuseeskirjade abil teatud andmekaitset kohtute või muude institutsioonide kaudu rakendada, on siiski näha, et niisugune kaitse on üldisem ja vähem tõhus kui riikides, kus asjaomane seadus on kehtestatud. Andmekaitse valdkonnas ei saa rääkida rahvusvahelistest (globaalsetest) standarditest, nii nagu seda saab teha näiteks sõnavabaduse puhul, vaid sellised laiema ulatusega standardid piirnevad küsimusega, millised olukorrad kuuluvad privaatsuse ehk eraelu puutumatuse kaitsealasse. Kuigi ELis nõutakse, et oleks loodud sõltumatu amet, kes vastutaks andmekaitse eest, ja kuigi andmekaitse ameteid on ka mujal maailmas, ei saa siiski väita, et see oleks universaalsetest õiguspõhimõtetest tulenev nõue. Erinevusi isegi suhteliselt sarnaste õigusruumide vahel on näha näiteks ELi ja Ameerika Ühendriikide vahel. Ameerika Ühendriikides puudub üldine andmekaitseseadus, reegleid luuakse eri valdkondades *ad hoc.* Kahel eri põhjusel on andmekaitse USAs vähem tõhusam kui ELis. Esiteks on USAs sõnavabadus veel rangemalt kaitstud kui Euroopas ja seetõttu on piirangud info kasutamiseks haruldased, isegi kui info sisu võib teatud määral privaatsust riivata. Teine erinevus on hoopis muul põhjusel: kuna puudub üldine andmekaitseseadustik ja sõltumatu järelevalve, siis on lihtsam riigi julgeoleku pärast piirata privaatsust.

Viimati nimetatud erinevust ELi ja USA vahel on märgata lahkarvamustes andmevahetuse kohta lennunduse alal, kus andmevahetus,[12] mida nõudis USA selleks, et anda lendamisõigus oma õhuruumi, oli vastuolus ELi andmekaitse reeglitega. Alates 2000. aastate algusest on seda teemat arutatud ja 2007. aastal jõuti kokkuleppele, mida muudeti 2011. aastal. Küsimus on pidevalt arutelu objektiks. Kuna moodne tehnoloogia on oma olemuselt globaalne, tuleb õigusruumi üle arutledes olla teadlik sellest, et kuigi saab viidata teatavatele olemasolevatele universaalsetele õigustele, on nende üksikasjalikum rakendamine riikides erinev. Rahvusvahelise avaliku õiguse eripära on see, et puudub ülemaailmne seadusandja, seega on kokkulepped ainus viis, kuidas jõuda rahvusvaheliste eeskirjade kehtestamiseni.

(Põhi)õigus andmekaitsele on tuletatud õigusest eraelu puutumatusele. Privaatsust ehk eraelu puutumatust on käsitletud olulistes rahvusvahelistes konventsioonides, nagu ÜRO inimõiguste ülddeklaratsioon[13] (artikkel 12)[14] ja Euroopa inimõiguste ja põhivabaduste kaitse konventsioon (EIÕK)[15] (artikkel 8)[16]. Privaatsusõiguse alla kuuluvad erinevad valdkonnad, näiteks posti, telefonikõnede ja muu kommunikatsiooni salastatuse kaitse; kodu puutumatus; kaitse laimu ja solvamise vastu; andmekaitse. Mida täpselt privaatsusõigus hõlmab, määrab juhtumipõhiselt kindlaks kohus. Seos andmekaitse ja privaatsuse vahel viitab sellele, et andmekaitse on oma olemuselt seotud just eraeluga ja õigusega ise otsustada, kellega ja

[12] PNR *Passenger Name Record Data.*
[13] http://vm.ee/et/uro-inimoiguste-ulddeklaratsioon.
[14] Artikkel 12 *Kellegi era- ja perekonnaellu, kodupuutumatusse või kirjavahetusse ei tohi meelevaldselt sekkuda ega teotada kellegi au ja head nime. Igaühel on õigus saada seaduselt kaitset sellise sekkumise või teotamise korral.*
[15] https://www.riigiteataja.ee/akt/78154.
[16] Artikkel 8 *(1.) Igaühel on õigus sellele, et austataks tema era- ja perekonnaelu ja kodu ning korrespondentsi saladust.*
(2.) Võimud ei sekku selle õiguse kasutamisse muidu, kui kooskõlas seadusega ja kui see on demokraatlikus ühiskonnas vajalik riigi julgeoleku, ühiskondliku turvalisuse või riigi majandusliku heaolu huvides, korratuse või kuriteo ärahoidmiseks, tervise või kõlbluse või kaasinimeste õiguste ja vabaduste kaitseks.

kuidas jagada enda eraeluga seotud andmeid. See seos piirab teatud määral andmekaitset, kuna need andmed, mis ei ole seotud eraeluga, või andmed, mille levitamine ei mõjuta eraelu puutumatust, ei ole kaitstud juhul, kui neile ei ole tagatud kaitset konkreetsete seadustega. Selliste andmete hulka võivad kuuluda näiteks äri- või muu tööalase tegevusega seotud andmed või andmed, mis on kergesti kättesaadavad ja mida seetõttu ei peeta inimese eraelu eriti palju mõjutavateks. Privaatsusõiguse ja andmekaitse seos tähendab ka seda, et riikides, kus puudub andmekaitseseadus, või olukordades, mille puhul selline seadus eri põhjustel ei kehti, võib siiski olla olemas teatud andmekaitse, mis tugineb privaatsusõigusele.

Privaatsusõigus, nagu ka suurem osa inimõigusi, ei ole absoluutne, vaid seda võib piirata teatud olukordades ja näiteks teiste õiguste pärast. Sõnavabaduse ja privaatsuse vahekorraga puutuvad kohtud tihti kokku.[17] Kohtud peavad kaaluma ühelt poolt põhjuseid teatud andmete avaldamiseks ning teiselt poolt seda, millist kahju selline avaldamine võib isikule tekitada. Tuleb leida proportsionaalne lahendus, mille puhul on arvesse võetud nii avalikkuse huve (kuhu kuulub vaba arutelu ja võimalus saada igasugust teavet) kui ka üksikisiku huve. Demokraatlikes sõnavabadust austavates riikides on vähe piiranguid sellele, mida meedias või mujal tohib avaldada. Eriti inimesed, kelledel on ühiskondlik positsioon, peavad taluma, et nende kohta tohib levitada ka negatiivset infot, teha karikatuure, kritiseerida nende tegevust, välimust, ütlusi jne.

Inimõiguste eesmärk on kaitsta olulisi põhiõigusi ja -vabadusi, eelkõige riigi või muude võimuorganite vastu, aga tagada ka see, et riik loob süsteemi selleks, et üksikisikud ei saaks teiste õigusi riivata. Privaatsuse valdkonnas on olemas kohtupraktikat näiteks Euroopa Inimõiguste Kohtust (EIK). Kohtupraktikast on üldiselt (iga õiguse piirangu suhtes) teada, et igasugune inimõiguste piirang peab olema seadusega reguleeritud, proportsionaalne ja demokraatlikus ühiskonnas vajalik. Seadused, mis ei ole proportsionaalsed ja vajalikud, võivad rikkuda inimõigusi ning võib tekkida olukordi, kus ei ole vajalikke seadusi või neid ei rakendata korrektselt. Moodsa meedia ja suhtlusvõrkudega seoses võib esineda mõlemat probleemi: ebasobivad seadused (või muud reeglid) või puudulik õigusraamistik. Kuna uute tehnoloogiate puhul on sageli raske ette näha, kas ja kuidas saab teatud tegevust seaduste ja muude reeglitega mõjutada (kas jurisdiktsiooni küsimuste tõttu, selle tõttu, et on raske rakendada olemasolevaid seadusi uutele ja keerukatele tehnoloogiatele, või muudel põhjustel), siis esineb mitmeid olukordi, kus inimestel on tunne (mida väljendab ka avalik arutelu), et olukord peaks olema reguleeritud, midagi peaks olema keelatud, teatud tegevust peaks saama peatada jne – kuigi tegelikult õigussüsteem ei oma selleks vajalikke vahendeid. Demokraatlikes riikides, mis austavad inimõigusi ja põhivabadusi, on siiski oluline, et see, mis ei ole seadustega keelatud, *on* lubatud ja mitte vastupidi (et iga tegevus peaks olema seadusega selgesõnaliselt lubatud).

[17] Riigikohus, õigusteabe osakond, Eve Rohtmets „Ajakirjandusvabaduse ja eraelu puutumatuse tasakaal Euroopa Inimõiguste Kohtu praktikas. Kohtupraktika analüüs", Tartu, märts 2014, www.riigikohus.ee.

PRIVAATSUSÕIGUS JA ISIKUANDMETE KAITSE EUROOPA LIIDU JA EESTI ÕIGUSES

EUROOPA LIIDU ANDMEKAITSEALANE ÕIGUS

ELi andmekaitse reeglid on esitatud Euroopa Parlamendi ja nõukogu 24. oktoobri 1995. aasta direktiivis 95/46/EÜ üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta[18]. Direktiivi eesmärk on kaitsta füüsiliste isikute õigusi ja vabadusi isikuandmete töötlemisel ja tagada andmekaitse põhimõtete kehtestamisega nende ühine kohaldamine liikmesriikides.

Direktiiv on hetkel üle vaatamisel,[19] eesmärgiga muuta reeglid moodsate tehnoloogiatega rohkem sobivaks ning samuti tagada, et edaspidi ei oleks nii suuri erinevusi riikide vahel, kui see mis hetkel on välja kujunenud. Viimati nimetatud põhjusel on plaanis kehtestada määrus direktiivi asemel. Määrus, mis on otseselt rakendatav igas liikmesriigis, ilma et seda viidaks siseriiklikkuse õigusesse üle, tagab suurema ühtsuse liikmesriikide vahel.

Peamisele andmekaitsedirektiivile lisaks on mitu spetsiifilisemat õigusakti, mis hõlmavad andmekaitset teatud olukorras. Siia kuulub direktiiv 2000/31/EÜ infoühiskonna teenuste teatavate õiguslike aspektide, eriti elektroonilise kaubanduse kohta siseturul[20] ning direktiiv 2002/58/EÜ, milles käsitletakse isikuandmete töötlemist ja eraelu puutumatuse kaitset elektroonilise side sektoris[21].

ELis kehtib ka direktiiv 96/9/EÜ andmebaaside kohta,[22] kuid see käsitleb andmebaase ainult autoriõiguse seisukohast ja ei tegele andmekaitsega. Andmetega tegeleb ka direktiiv 2003/98/EÜ avaliku sektori andmete taaskasutamise kohta[23]. See direktiiv mõjutab kaudselt andmekaitse olukorda, kuna selles sätestatakse, et avaliku sektori andmeid tohib kasutada ärilistel eesmärkidel, luues seega andmetest lisaväärtust. Direktiiv viitab andmekaitsedirektiivile ja ei loo uusi reegleid, selles eeldatakse, et andmed on kaitstud. Lisaks on ka olemas Nõukogu raamotsus 2008/977/JSK kriminaalasjades tehtava politsei- ja õigusalase koostöö raames töödeldavate isikuandmete kaitse kohta ja muid mittesiduvaid akte lihtsustamaks koostööd liikmesriikide vahel.

---

[18] Euroopa Parlamendi ja nõukogu direktiiv 95/46/EÜ, 24. oktoober 1995, üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta (EÜT L 281, 23.11.1995, lk 31).

[19] http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm.

[20] Euroopa Parlamendi ja nõukogu direktiiv 2000/31/EÜ, 8. juuni 2000, infoühiskonna teenuste teatavate õiguslike aspektide, eriti elektroonilise kaubanduse kohta siseturul (direktiiv elektroonilise kaubanduse kohta) (EÜT L 178, 17.7.2001, lk 1).

[21] Euroopa Parlamendi ja nõukogu direktiiv 2002/58/EÜ, 12. juuli 2002, milles käsitletakse isikuandmete töötlemist ja eraelu puutumatuse kaitset elektroonilise side sektoris (eraelu puutumatust ja elektroonilist sidet käsitlev direktiiv) (EÜT L 201, 31.7.2002, lk 37).

[22] Euroopa Parlamendi ja nõukogu direktiiv 96/9/EÜ, 11. märts 1996, andmebaaside õiguskaitse kohta (EÜT L 77/20, 27.3.1996, lk 459).

[23] Euroopa Parlamendi ja nõukogu direktiiv 2003/98/EÜ, 17. november 2003, avaliku sektori valduses oleva teabe taaskasutamise kohta (ELT L 345, 31.12.2003, lk 90).

ELi kohtupraktikas on aastate jooksul olnud mitmeid kohtuasju andmekaitse kohta, mille kaudu on loodud kindlamad raamid direktiivide tõlgendamiseks. Nende kohtuasjade kaudu on ka selgelt näha olnud, et eri liikmesriikides valitsevad erinevad arusaamad, mis on üks põhjus, miks ELi andmekaitsereform on vajalik. Eriti huvitav on otsus kohtuasjas C-131/12, mis tehti 2014. aastal ja mis käsitles õigust olla unustatud. Kokkuvõttes otsustas Euroopa Kohus, et Google peab maha võtma oma otsingu tulemustest teatud info, mis võib isikutele negatiivne olla, kui ei ole olulist põhjust avalikkuse huvides, et see info oleks kättesaadav. Kuigi esialgu võib selline reegel tunduda andmekaitse ja privaatsuse põhimõtetega kooskõlas olev, on veidi sügavama analüüsi puhul märgata erinevaid ohte. Näiteks on eraettevõttel Google võimalus ajalugu kustutada. Et selline tegevus ei oleks liiga ulatuslik, on loodud üsna range süsteem, mis olukordades saab taotleda andmete kustutamist. Liiga laiaulatuslik andmete kustutamine ohustaks sõnavabadust ja inimõiguses sisaldavat õigust otsida informatsiooni ja omandada teavet, samas kui kustutamise nõuded on väga ranged, võib see tähendada, et selle tegevuse reaalne tähendus kaob. Lisaks kehtib selline süsteem peamiselt ELis, kuna mujal maailmas ei ole siiamaani sarnaseid otsuseid vastu võetud ja Interneti globaalse olemuse tõttu võib sama info mujalt kätte saada. See võib tähendada ka, et tegelikult ei ole ELi kohus muud teinud, kui tekitanud vale kindlustunde ebameeldiva andmete ajaloo kustutamise võimaluse suhtes, mis võib viia isegi selleni, et inimesed on veel vähem ettevaatlikud oma isiklike andmete levitamisel.

Andmekaitseseadustes ning ELi direktiivis on seletatud lahti terminid, mida kasutatakse õigusaktides. Andmed, mida kaitstakse, on isikuandmed, mis sisaldavad igasugust teavet tuvastatud või tuvastatava füüsilise isiku kohta, arvestades, et tuvastatav isik on isik, keda saab otseselt või kaudselt tuvastada, eelkõige isikukoodi põhjal või ühe või mitme tema füüsilisele, füsioloogilisele, vaimsele, majanduslikule, kultuurilisele või sotsiaalsele identsusele omase joone põhjal[24]. Andmed võivad olla rohkem või vähem delikaatsed, aga kõik andmed tuvastatud isikute kohta on seaduse mõistes isikuandmed ja neid tuleb töödelda seadustes ettenähtud korras.

Andmekaitse-reeglitele lisaks on ka teisi õigusvaldkondi, mis mõjutavad andmetega seonduvat, eriti moodsa IKT, näiteks suhtlusvõrgustikega seoses. Siia kuulub näiteks tarbijakaitseõigus. Kuna e-kaubanduse ja e-teenuste puhul ei ole tehingute osapooled samal ajal samas kohas – neil puudub isiklik kontakt –, on eriti tähtis, et tehingud on arusaadavad ja tarbijad on teadlikud, millega nad eri tehingute kaudu nõustuvad. Eelkõige kuna e-teenuste puhul on võimalikud igasugused lisateenused, mis on ainult osaliselt seotud algse teenusega, siis peab tagama võimalikult kindlalt, et igasugune nõusolek on teadlik. Seda saab teha näiteks nõudmise kaudu, et kasutustingimused on kättesaadavad ning et veebilehel peavad inimesed kinnitama, et nad on tingimustega tutvunud. Lisaks on näiteks ELis keelatud automaatselt valitud lisateenused, vaid nõutakse nende tellimiseks mingit tegevust, mis küll tavaliselt piirdub ainult linnukese panemisega ettenähtud kohta veebilehel. Tegelikult on muidugi võimatu niisuguste meetmetega garanteerida, et isikud reaalselt on teadlikud ning nende nõusolek on teadlikult ja vabatahtlikult antud. Samas on raske ette kujutada, kuidas saaks õigussüsteem seda muul viisil teha: lõpuks on siiski isiku enda vastutus oluline ja teadlikkust peab püüdma suurendada hariduse, kampaaniate, meedia jms kanalite kaudu.

[24] Direktiivi 95/46/EÜ artikkel 2. Mitmed andmekaitseseadused, eelkõige ELis aga ka mujal, kasutavad väga sarnast terminoloogiat.

EESTI ANDMEKAITSE ÕIGUSSÜSTEEM

Eesti põhiseadus

Eesti Vabariigi põhiseaduses on mitu paragrahvi privaatsuse eri aspektide kaitseks. Paragrahvis 26 on sätestatud perekonna- ja eraelu puutumatus ning paragrahvis 33 kodu puutumatus. Paragrahvis 42. alusel Riigiasutused, kohalikud omavalitsused ja nende ametiisikud ei tohi Eesti kodaniku vaba tahte vastaselt koguda ega talletada andmeid tema veendumuste kohta. Kommunikatsiooni kanalite saladus on kirjas paragrahvis 43. Otseselt on teabe ligipääs ja andmekaitse kindlustatud paragrahviga 44.

§ 44. *Igaühel on õigus vabalt saada üldiseks kasutamiseks levitatavat informatsiooni.*

Kõik riigiasutused, kohalikud omavalitsused ja nende ametiisikud on kohustatud seaduses sätestatud korras andma Eesti kodanikule tema nõudel informatsiooni oma tegevuse kohta, välja arvatud andmed, mille väljaandmine on seadusega keelatud, ja eranditult asutusesiseseks kasutamiseks mõeldud andmed.

Eesti kodanikul on õigus seaduses sätestatud korras tutvuda tema kohta riigiasutustes ja kohalikes omavalitsustes ning riigi ja kohalike omavalitsuste arhiivides hoitavate andmetega. Seaduse alusel võib seda õigust piirata teiste inimeste õiguste ja vabaduste ning lapse põlvnemise saladuse kaitseks, samuti kuriteo tõkestamise, kurjategija tabamise või kriminaalmenetluses tõe väljaselgitamise huvides.

Kui seadus ei sätesta teisiti, siis on käesoleva paragrahvi lõigetes kaks ja kolm nimetatud õigused võrdselt Eesti kodanikuga ka Eestis viibival välisriigi kodanikul ja kodakondsuseta isikul.

Õigus kontrollida enda kohta käivat informatsiooni ehk nn informatsioonilise enesemääramise õigus on isikuandmete kaitse põhimõtete alus.

Isikuandmete kaitse seadus ja muud õigusaktid

Eestis on peamine andmekaitseseadus isikuandmete kaitse seadus, mis võeti vastu 15. veebruaril 2007[25]. Seadus sätestab isikuandmete töötlemise tingimused ja korra, riikliku järelevalvekorra isikuandmete töötlemise üle ja vastutuse nõuete rikkumise eest.

Seadus tugineb ELi direktiivile ja on sellega kooskõlas. Nagu eespool mainitud, on üks ELi andmekaitsereformi mõte see, et peaks looma direktiivi asemel määruse, mis oleks otse kohaldatav liikmesriikides. Samas oleksid ka pärast niisugust reformi mitmed põhimõtted, mis on nii ELi kui ka Eesti õiguses juba praegu olemas, jätkuvalt kehtivad.

Isikuandmete kaitse seaduse paragrahvis 1 on viidatud eraelu puutumatusele ning ka isiku põhiõigustele ja -vabadustele üldisemalt.

[25] RT 2007, 24, 127.

Seaduses on sätestatud isikuandmete töötlemise põhimõtted, mida isikuandmete vastutav ja volitatud töötleja on kohustatud järgima. Oluline on ka, et vastutav isik oleks määratud (paragrahv 7). Andmete töötlemisel peab isikuandmete töötleja järgima peamisi andmekaitse põhimõtteid: seaduslikkuse, eesmärgikohasuse, minimaalsuse ning kasutuse piiramise põhimõtet, samuti andmete kvaliteedi, turvalisuse ning individuaalse osaluse põhimõtet. Viimane põhimõte tähendab, et andmesubjekti tuleb teavitada tema kohta kogutavatest andmetest, talle tuleb võimaldada juurdepääs tema kohta käivatele andmetele ja tal on õigus nõuda ebatäpsete või eksitavate andmete parandamist. Seda õigust on teiste seaduse sätetega täpsemalt rakendatud. Eesmärgipärasuse ja kasutuse piiramise põhimõtted sätestavad, et isikuandmeid võib koguda üksnes määratletud ja õiguspäraste eesmärkide saavutamiseks ning isikuandmeid võib muudel eesmärkidel kasutada ainult andmesubjekti nõusolekul või selleks pädeva organi loal.

Kuigi üldiselt on isikuandmete töötlemine lubatud andmesubjekti nõusolekuga, on siiski ka olukordi, kus andmeid saab töödelda ilma nõusolekuta. Need olukorrad on seaduses ära toodud (paragrahv 14), näiteks seaduses sätestatud juhtudel või seadusest tulenevate ülesannete täitmiseks, isikuga sõlmitud lepingu täitmiseks, ülekaaluka avaliku huvi korral jne.

Seaduse paragrahvis 5 sätestatakse, mis on isikuandmete töötlemine. Tekst on võetud ELi direktiivist ja sätestab, et töötlemine on iga isikuandmetega tehtav toiming, sealhulgas isikuandmete kogumine, salvestamine, korrastamine, säilitamine, muutmine ja avalikustamine, juurdepääsu võimaldamine isikuandmetele, päringute teostamine ja väljavõtete tegemine, isikuandmete kasutamine, edastamine, ristkasutamine, ühendamine, sulgemine, kustutamine või hävitamine, või mitu eelnimetatud toimingut, sõltumata toimingute teostamise viisist ja kasutatavatest vahenditest. Teatud olukordade suhtes, näiteks isiklikul otstarbel enda andmete töötlemine, seadust ei kohaldata. Üldiselt on definitsioon töötlemise kohta nii lai, et see hõlmab igat andmete kasutamist.

Isikuandmete kaitse seadus annab väga üldised suunised isikuandmete kaitsmiseks (paragrahvid 25 ja 26). Täpsemalt on Eesti valitsusasutuste ja kohalike omavalitsuste poolt kogutavate andmete turvataseme või turvaklassi hindamine ja asjakohaste turvameetmete määramine ning rakendamine lepitud kokku erinevate Vabariigi Valitsuse määrustega[26]. Suuremates ja andmeturbega kokkupuutuvates ettevõtetes rakendatakse vabatahtlikult või valdkonnapõhistest õigusaktidest ja nõudmistest tulenevalt mõnda rahvusvaheliselt tunnustatud turbestandardit[27] ja -metoodikat. Andmete turvataseme määramine on oluline ja sellest sõltub, kuidas andmeid edaspidi kaitstakse. See tähendab, et see, kes otsustab eri andmete üle, peab olema selleks pädev.

Sideettevõtjate vastutus andmete eest tuleneb ka elektroonilise side seadusest[28] (10. peatükk andmete turvalisuse ja kaitse kohta). Sideettevõtjal on kohustus tagada

[26] Näiteks Vabariigi Valitsuse määrus infosüsteemide turvameetmete süsteemi kohta (RT 1, 2007, 71, 440) ja infoturbe juhtimise kohta (RT I, 19.03.2012, 4), hädaolukorra seaduse alusel kehtestatud Vabariigi Valitsuse määrus elutähtsate teenuste infosüsteemide ning nendega seotud infovarade turvameetmete kohta (RT I, 20.03.2013, 7).

[27] Näiteks EVS-IEC/ISO 27001 vms standardite perekondi.

[28] RT I 2004, 87, 593.

andmete kaitse ja töödelda neid nii, et ei rikuta andmekaitse põhimõtteid. Isikuandmetega seotud rikkumise korral on sideettevõtja kohustatud sellest esimesel võimalusel teavitama Andmekaitse Inspektsiooni (paragrahv 102). Osalt on elektroonilise side seaduse eesmärk tagada, et sideettevõtjad – kes puutuvad ju pidevalt kokku andmetega – tagaksid andmekaitse põhimõtete järgimise oma tegevuses. Elektroonilise side seadus sisaldab ka eri andmete suhtes konkreetseid reegleid, näiteks kliendi asukoha andmete kohta (paragrahv 105). Peamine reegel on, et sellised andmed peab enne töötlemist muutma anonüümseks, vastasel juhul peab olema andmesubjekti – kliendi – nõusolek andmete töötlemiseks.

Lisaks on andmekaitset nimetatud eri määrustes, mis käsitlevad spetsiifilisi andmetöötlemise süsteeme.

Järelevalve

ELi andmekaitsesüsteemi üks oluline osa on, et igal riigil peab olema andmekaitse inspektsioon või muu sarnane sõltumatu amet, millel on pädevus tagada järelevalve andmekaitse olukorra üle riigis, kaasa arvatud valitsuse organite juures. Inspektsioon peaks võtma vastu kaebusi ning ka ise alustama uurimist ning lisaks on see tavaliselt organ, kes annab lubasid andmete töötlemiseks – selle kaudu uurides kavandatavaid süsteeme. Ka mitmes riigis väljaspool ELi on loodud andmekaitseametid, mis on mitmel juhul ELi reeglitest eeskuju võtnud. Samuti on võimalik, et mingi muu asutus, näiteks ombudsman, tegeleb ka andmekaitsega. Oluline on, et järelevalve on tõhus ning et on selge, kuhu peaks pöörduma andmekaitse probleemidega. Kuna ameti loomise eesmärk on soovitada ja õpetada, kuidas andmetega korralikult ümber käia, siis on ka oluline, et ameti tegevus oleks suures osas avalik ja selle otsused ning soovitused kergesti kättesaadavad. Selle kaudu luuakse hea tava. Ka probleemide korral juhtub sageli, et inspektsioon ei otsusta muud, kui et viitab probleemidele ja soovitab, mida tuleks teha teistmoodi.

Eesti Andmekaitse Inspektsiooni põhimääruses on sätestatud inspektsiooni põhiülesanded:

§ 9. Inspektsiooni põhiülesanded

Inspektsiooni põhiülesanded on:

1) riikliku järelevalve teostamine inspektsiooni tegevusvaldkonda reguleerivatest õigusaktidest tulenevate nõuete täitmise üle ja vajadusel riikliku sunni rakendamine;

2) osalemine oma tegevusvaldkonda puudutavate õigusaktide väljatöötamisel ning ettepanekute tegemine nende muutmiseks ja täiendamiseks;

3) osalemine oma tegevusvaldkonnaga seotud poliitika, strateegia ja arengukavade väljatöötamisel;

4) oma tegevusvaldkonnaga seotud projektide ettevalmistamine ja elluviimine, sealhulgas osalemine rahvusvaheliste projektide ettevalmistamisel ja läbiviimisel;

5) osalemine oma tegevusvaldkonda puudutavate rahvusvaheliste töögruppide ja organisatsioonide töös.

Andmekaitse Inspektsioonil on nii järelevalveosakond kui ka üldosakond. Andmekaitse ametite üks tähtis roll on teadvustamine ning ennetav töö. Andmekaitse Inspektsiooni

üldosakond tegeleb teavitustöö, rahvusvahelise koostöö ja muu sarnase tegevusega[29]. Otsused on veebis kättesaadavad koos juhistega ja üldise infoga eraelu kaitse ning avaliku teabe kohta. Juhiseid on väga palju eri spetsiifiliste teemade kohta,[30] näiteks infoturve ja isikuandmete kaitse väikeettevõttes või isiklikud mobiilsed seadmed töökeskkonnas. Juhised ja otsused koos aitavad luua tõhusama andmekaitsesüsteemi, mis peaks olema ka mittespetsialistidele arusaadav.

Andmekaitse Inspektsiooni kodulehel on kättesaadav teave selle kohta, kuidas tuleb käituda, kui esitada kaebus andmete töötlemise kohta[31]. Samuti on esitatud erinevate pöördumiste näidised koos selgituste, näidisvormide ja muu vajaliku informatsiooniga. Tekst on selge ja näidised aitavad isikutel esitada olulist infot. Inspektsiooni tegevus on suunatud rikkumise lõpetamisele, nagu seda kodulehel kirjeldatakse. Teatud juhtumitel võib siiski olla vaja pöörduda kohtu poole. Andmete väärkasutusest võib teavitada ka juhul, kui see otseselt isikut ei puuduta. Kuigi vajalik info ja protseduurid on olemas ja neid on selgelt kirjeldatud, puuduvad paljudel inimestel teadmised, mida peaks tegema andmete kaitseks, kui on hirm, et isikuandmete töötlemisega on probleeme[32]. Inspektsioon saaks ehk rohkem teavitada meedia ja muude sarnaste kanalite kaudu, aga sellele lisaks on raske ette näha enamat, kui inimesed ise ei otsi informatsiooni, mis on vabalt kättesaadav.

LÕPETUSEKS VÄLJAKUTSETEST ANDMEKAITSEÕIGUSELE

Inimkonna ajaloos on toimunud pidevalt muutusi nii ühiskonnas, tehnoloogias, praktilises elus kui ka tõekspidamistes. Samas on viimastel aastakümnetel need muutused olnud kiiremad kui varem ja muutnud meie igapäevaelu suuremal määral kui varasematel aegadel. See tähendab väljakutset õiguste rakendamisele ja seadusandlusele. Keerulistel aegadel, kui inimesed ei saa hästi aru, kuidas tegutseda pidevate uute tegevuste, tehnoloogiate ja kontaktide taustal, oodatakse tuge väljastpoolt, kellegi või millegi poolt – näiteks seadusandluse ja selle rakendamise poolt. Sellist suundumust on märgata privaatsuse ja andmekaitse valdkonnas, kus uued suhtlustehnoloogiad ja -meetodid on kindlasti toonud kaasa uusi väljakutseid ja ohte. Samas on olemasoleval seadusandlusel raske nende väljakutsete ja ohtudega toime tulla ja mitmel põhjusel on keeruline luua uusi, sobivamaid seadusi. Tegelikkuses on nii, et inimese enda vastutus on suurem just ajal, mil ta ootab suuremat tuge.

Eestis, nagu enamikus ELi liikmesriikides, on eraelu seadusega kaitstud ning andmekaitseks on loodud reeglid ning järelevalvesüsteemid. Sellest hoolimata andmeid kuritarvitatakse või need satuvad valedesse kätesse. Kuigi teatud reforme on kindlasti vaja, et paremini kajastada moodsaid tehnoloogiad, ei saa siiski väita, et andmekaitsereeglistikuga oleks suuremaid probleeme. Pigem on raske ükskõik missuguseid reegleid rakendada nii kiiresti muutuvas ning nii rahvusvahelises keskkonnas kui on seda näiteks moodsad

[29] http://www.aki.ee.
[30] http://www.aki.ee/et/eraelu-kaitse/juhised.
[31] http://www.aki.ee/et/inspektsioon/poordu-inspektsiooni-poole.
[32] Seda näitas avaliku arvamuse küsitlus, mis on käesoleva uuringu osa.

suhtlusvõrgustikud, eriti kuna inimesed kogu aeg oma käitumise kaudu teevad kättesaadavaks aina rohkem infot enda kohta aina suuremale ringile.

Nähtus, mida võime ka läbi ajaloo näha, on, et põlvkondadel on erinevad arusaamad ja tõekspidamised ning ka nende oskused on erinevad. Ka selles suhtes on hiljaaegu olnud muudatused kiiremad. Andmekaitse ja privaatsuse osas tähendab see seda, et noored inimesed, kes on kasvanud üles interaktiivsete suhtlustehnoloogiatega, mille kaudu on väga palju isiklikku informatsiooni kergesti ja laialdaselt kättesaadav, näevad privaatsust teistmoodi kui vanemad inimesed. Seadusandlus ja selle rakendamine on loodud varasemate tõekspidamiste alusel. Õigussüsteemi üks ülesanne on mõjutada inimeste käitumist ja ka nende arusaama ühiskonnast ja selle reeglitest, kuid selline mõjutamine peab toimuma mingil heal ja vajalikul eesmärgil. Küsida tuleb, et kui inimesed ei näe ja ei tunneta ohtu, siis kas neid tuleb siiski kaitsta?

Isiku enda vastutuse kontekstis on õiguslikult oluline, kas on antud nõusolek mingiks tegevuseks või toiminguks ja kas see nõusolek oli vabatahtlik ja teadlik. On ka olukordi, kus isegi nõusolekuga ei ole eri tegevused lubatud. Tegevus kui selline võib olla keelatud kui üldiselt kahjulik või professionaalse eetikaga vastuolus olev või andmete kasutus võib riivata kolmandate isikute privaatsust. Palju tavalisemad on aga olukorrad, kus formaalselt võib küll nõusolek olla antud, aga tegelikult see ei olnud vabatahtlik ega teadlik. Põhjuseks võib olla, et inimene ei saanud aru, millele ta nõusoleku andis, kuna olukord oli nii keeruline, informatsioon puudulik või inimesel puudusid reaalsed võimalused adekvaatselt olukorrast aru saada. Põhjus võib aga peituda ka hoopis selles, et kuigi inimene sai aru ja ei oleks tahtnud anda nõusolekut, siis tegelikult ei olnud tal valikuvõimalust, kuna vastasel juhul – nõustumata teatud tegevusega – oleks jäänud ta ilma millestki muust, mis on tema jaoks oluline. Näiteks on teenuseid, mille tarbimiseks peab olema Facebooki või Twitteri konto, mis tähendab, et nendest võrgustikest loobumine tähendab ka teatud teistest teenustest loobumist (nt teatud elektrooniliste ajakirjade jms lugemine või kommenteerimine). Moodsate infotehnoloogiatega seoses tuleb esile mitmeid olukordi: nii olukordi, kus inimesed ei saa situatsioonist aru, kuna tehnoloogia on nii kompleksne, kui ka olukordi, kus tehnoloogiad on muutunud nii oluliseks, et nendest kõrvalehoidumine teeb elu nüüdisaja ühiskonnas väga raskeks.

Isikute enda vastutus ei seisne mitte ainult selles, et ollakse teadlik eri kasutustingimustest ja antakse nõusolek ainult selliseks andmete kogumiseks või töötlemiseks, mida tegelikult ollakse valmis lubama, vaid seisneb ka selles, et praktiliselt käitutakse nii, et minimeerib riske, et kus andmeid ei saa kaitsta. Tihti leitakse probleemile pigem mitteelektrooniline seletus, st probleem ei ole tehnoloogias, vaid selles, kuidas seda kasutatakse – kas või niisugune lihtne seletus, et keegi jättis ukse lahti ruumi, kus oli avatud tundlike andmetega arvuti, või kaotas mälupulga koos andmetega[33].

Tehnoloogia võib hoopis tõhustada andmete kaitsmist, näiteks selle kaudu, et annab märku, kui andmeid väärkasutatakse. Igal juhul peab andmekaitse aspekt olema infosüsteemide hindamise osa nii selle kaudu, kuidas süsteem aitab tagada paremat andmekaitset, kui ka selle kaudu, missuguseid võimalikke ohte see esile toob ja kuidas nende vastu võidelda

[33] Näited http://ico.org.uk/what_we_cover/handling_complaints.

tõhusalt ja samas proportsionaalselt[34]. Viimasel ajal viidatakse tihti (sealhulgas uues ELi andmekaitsemääruses) "*Privacy by Design*" ehk "Lõimitud andmekaitse" põhimõttele. Selle põhieesmärk on, et andmekaitse peaks olema algselt sisse ehitatud IT-süsteemide disaini ja arhitektuuri ning integreeritud äritegevusse[35].

Niisiis, kui tehnoloogia esitab ühelt poolt uusi väljakutseid, siis võib see ka teiselt poolt riske maandada. Kuigi identiteedi vargust esineb kogu maailmas, siis on see siiski kõige tavalisem nendes riikides, kus puudub ühtne isikute identifitseerimise süsteem isikukoodi ja/või dokumendi abil. See tähendab, et e-riik või elektroonilised andmebaasid ning ID-kaardid ei pruugi kaasa tuua suuremaid ohte selles valdkonnas, vaid hoopis vastupidi. Andmevargusi käsitlevate USA seaduste võrdlevad uuringud on näidanud, et tehnoloogia muudab sellised vargused raskemaks, kuna teeb kurjategijate jaoks keeruliseks jõuda soovitud tulemusteni[36]. Selliste meetmete hulka kuuluvad näiteks infosüsteemides tulemüürid (*firewalls*), mis piiravad väljastpoolt juurdepääsu ja kontrollivad võrguliiklust, loogilised juurdepääsuõigused ja toimingute logid tagamaks, et infosüsteemis ei saa volituseta andmeid muuta, jne. Osa neist meetmetest aitavad kaitsta uute riskide eest, mida tehnoloogia ise on loonud. Tehnoloogiat on aga võimalik rakendada ka selleks, et teha toiminguid elektroonilises maailmas hoopis turvalisemaks kui need on nn pärismaailmas. Küll on see suhtumine palju üldistes hoiakutes kinni ja tekitab endiselt vastakaid arvamusi ning vaidlusi, näiteks Eestis laialt kasutatav e-valimiste süsteem või ID-kaart ei ole leidnud heakskiitu mõningates teistes riikides.

Tehnoloogiate kasutamine ja automatiseeritud andmetöötlus võib anda lisaks teadmisi, mida oleks võimatu ilma nende abita saavutada, ja seega võib rikkuda õigustatud ootusi andmete töötlemise ulatuse ja eesmärgipärasuse suhtes. Illustratsiooniks: kui isik näiteks jalutab sõbraga tänaval ja sööb jäätist, on igal möödaminejal võimalik saada infot: mis tal seljas on, mis jäätist ta sööb, kellega räägib, kuidas välja näeb ja võib-olla ka seda, millest ta räägib. Kui isik ei taha, et seda kõike teada saadaks, peab ta muutma oma käitumist. Ei saa ju nõuda, et inimesed ei tohi vaadata, mis avalikus ruumis toimub. Samas on õigustatud ootus, et magamistoas – isegi kui see on üürikorter või hotellituba – või riietusruumis ei ole kaameraid ega möödaminejatel vaba vaade. Samu põhimõtteid peab rakendama elektroonilises keskkonnas. Siinkohal tuleb aga silmas pidada, et tehnoloogiad (näiteks nn näotuvastuse (*face recognition*) tehnoloogia, mida kasutab nt Facebook[37]) võimaldavad tänaval jalutavast inimesest rohkem teada saada kui ainult niisama vaadates. Tuleb analüüsida, kas selline teadmine võib kuidagi isikut ja tema privaatsust riivata, ja kui see on nii, siis kaaluda, kas seda saab takistada. Sellist analüüsi küll tehakse juba mitmeid aastaid nii akadeemilises ja üldises arutelus, ettevõtted ise kui ka teatud määral kohtud, aga siiski

[34] Näide uuringu kohta: „Opinion of the European Data Protection Supervisor on the Proposals for a Regulation establishing an Entry/Exit System (EES) and a Regulation establishing a Registered Traveller Programme (RTP)", 18 July 2013.
https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2013/13-07-18_Smart_borders_EN.pdf.

[35] Lõimitud eraelukaitse põhimõtete kohta loe täpsemalt:
http://www.privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples-estonian.pdf.

[36] M. Anandarajan, R. D´Ovidio, A. Jenkins (2013) „Safeguarding consumers against identity-related fraud: examining data breach notification legislation through the lens of routine activities theory": *International Data Privacy Law* 2013 Vol. 3, No. 1 (51-60): lk 53.

[37] Vaata vaidluse kohta lähemalt näiteks: http://www.theguardian.com/technology/2014/may/04/facial-recognition-technology-identity-tesco-ethical-issues.

peab nentima, et ei ole veel üldist tunnustatud arusaama tehnoloogia rakendamise piiride kohta.

Infotehnoloogia on toonud kaasa ühiskonnas suuri muudatusi mitmes vallas; üks enim mõjutatud ala on meedia. Nii ajalehtede kui ka ringhäälingu ja ka laiemalt ajakirjanduse kui elukutse jaoks on moodne meedia ja selle otsekohesus ning globaalne levik tähendanud täiesti uut tegelikkust. Privaatsust mõjutab see mitmel moel, näiteks selle kaudu, et enam ei saa arvestada riigipoolse regulatsiooni (ringhääling) või eneseregulatsiooniga (peamiselt trükimeedia) ja ajakirjanduse professionaalse eetikaga, et luua raame selleks, mida tohib meedias näidata ja kuidas. Tavalised inimesed saavad reaalajas levitada infot ülemaailmselt väga vähese kulu ja tööga. Sõnavabadusele võib see olla väga hea, kuna üha enam infot levib üha enamatele inimestele, aga samas toob see esile teravamalt kui kunagi varem kõik need olukorrad, kus sõnavabadus ja muud inimõigused ja -vabadused – eelkõige privaatsusõigus – võivad olla vastuolus.

Tehnoloogiad on muutnud seda, kes on olulised osalised olemasolevate reeglite rakendamisel. Meedia suhtes on juba mainitud, kuidas osalejate ring on palju suurem ja ebamäärasem kui ainult mõned aastakümned varem. Üldiselt ja peaaegu igas ühiskonnas ja suuremas osas maailma riikides on lisaks toimunud veel see muudatus, et erasektoril on väga suur roll. Interneti teenusepakkujad, kes on olulised ju selleks, et suur osa tänapäeva riigist üldse toimida saaks, on suuremalt osalt eraettevõtted. Olulised suhtlusvõrgustikud kuuluvad erafirmadele. Olukord infotehnoloogia vallas ei ole ainulaadne, kuna ka näiteks transpordi- ja energeetikavaldkonnas on palju enam eraettevõtlust kui umbes 30 aastat tagasi ja nii on see suuremas osas maailmast. Eraettevõtted on üldiselt efektiivsemad, suudavad kiiremini ja tõhusamalt uuendusi läbi viia ja pakuvad valikuvõimalusi üksikisikutele, nii et seda arengut tuleb tervitada. Samas tähendab see ka väljakutseid õigussüsteemile, kuna riigid peavad suutma rakendada tõhusalt õigusnorme ettevõtete vastutuse suhtes ning suutma ka vältida, et teatud ettevõtted muutuvad nii võimsaks, et saavad negatiivselt turgu mõjutada ja seeläbi piirata neidsamu eeliseid, mida turg endaga kaasa toob. Eriti keeruline võib õiguslik olukord olla sellepärast, et suured ettevõtted on tihti rahvusvahelised ja tekivad jurisdiktsiooni küsimused.

Loetletud teemad tähendavad, et andmekaitse ja privaatsuse kaitse nüüdisaegses kõrgtehnoloogilises ühiskonnas on keeruline ja ei ole imekspandav, et seda arutatavad väga palju ülemaailmselt, nii poliitikud, teadlased, kodanikuühiskond ja ka meedia esindajad. Debatist on ka näha, et ei ole mingit ühtset vastust, kuidas nende eri väljakutsetega tegeleda, või isegi selgeid suundi. Huvitav näide selle kohta on ELi kohtuotsus Google'i vastu, mis käsitles õigust olla unustatud, mille taustaks on privaatsuse kaitse ja mille suhtes on mitmed inimõiguste organisatsioonid väga kriitilised, kuna kardavad, et see ohustab sõnavabadust.

Tuleb arvestada sellega, et inimesed ei ole nii teadlikud kui nad peaksid olema, et tõeliselt ja pikaajaliselt hinnata ohte andmekaitsele, mis võivad suhtlusvõrgustike ja moodsa meedia kaudu esile kerkida. Sellepärast on raske ainult isiku enda vastutusele tugineda. Samas on oluline mitte üle hinnata, mida saab seadusandluse abil teha. Õigussüsteemi kaudu saab näiteks luua raamistiku ettevõtete vastutusele, kehtestada teatud tingimused ettevõtete tegevuse jaoks, et see oleks nii ohutu kui võimalik, ja juhuks, kui midagi läheb valesti, siis on

meetmeid sellega tegelemiseks. Aga õigus koos ametliku järelevalvega on ainult üks osa terviklahendusest. Siia tervikpilti kuulub kindlasti ka uus viis, kuidas hinnatakse privaatsust: moodne tehnoloogia ei pea tähendama privaatsuse lõppu, aga selle ümberhindamist tähendab see kindlasti.