

# Terrorismi mõju e-õigusele

28. detsember 2001 - 23:15 Autor: [Eneken Tikk](#)

Etteruttavalt võiks 11. septembri sündmuste mõju e-õiguse arengule nimetada praeguses vahekokkuvõttepunktis positiivseks. Eeskätt pöördus avalikkuse ja võimude tähelepanu traagiliste sündmuste järel senisest teravamalt küberkeskkonna turvalisuse problemaatikale ning Interneti vahendusel aset leida võivatele mustadele stsenaariumitele. Et küberterrorism ja -kuritegevus ka varem e-õiguses käsitlust on leidnud, siis ei ole teemade ring iseenesest oluliselt laienenud.

Kui esimene õk 11. septembri sündmustest sai mööda, algas mitmel tasandil aktiivne tegevus sarnaste juhtumite edasiseks ennetamiseks ning süüdlaste väljaselgitamiseks. Sellesse pealtnäha lihtsasse raami on USA valitsus suutnud mahutada vähemalt kaks avalikkuse emotsioone kütnud seaduseelnõud ning hulga turvameetmeid, millest arvestatav osa on suunatud ka Internetis toimuva jälgimisele.

Üks on kindel - USA-s toimunu mõjutab vähemalt kaudselt e-õiguse arengut kogu maailmas. Ehkki Euroopa e-õigusruumis pole seni erilisi muudatusi tehtud, on kõik see, mis Ameerika Ühendriikides kehtima hakkab, ka Interneti siinsele kasutajaskonnale kui mitte kohustuslik, siis vähemalt teadvustamist vajav. Kuivõrd jurisdiktsiooni üldpõhimõtted on e-õiguse valdkonnas traditsioonilisest veidi erinevad, siis tuleb igapäev valmis olla ebameeldivusteks ka seal, kust neid ehk oodatagi ei oska.

Suurematest saavutustest on tegelikult veel veidi vara rääkida. Üksnes asjaolu, et küberküsimused senisest enam avalikkuse tähelepanu pälvivad, ei võimalda teha päris vettpidavaid järeldusi kõigi võimalike tagajärgede kohta. Olgu siinkohal toodud lihtsalt mõned e-õigusega seonduvad aspektid.

## **E-etikareeglite võidukäik?**

Ebay võttis võimude otsese sekkumiseta maha mitusada teadet oksjoneist ja peatas mitmed kasutajaõigused, et takistada inimestel WTC tragöödia arvelt tulu teenida. 24 tunni jooksul peale rünnakut oli Ebay vahendusel siiski võimalik osta ja müüa pilte kokkuvarisevatest tornidest ja muid sellekohaseid "meeneid". Ebay sulges oktoobrini ka kõigi muude WTC-d ja Pentagoni käsitlevate linkide kasutamise portaali kaudu.

Püsivat e-etika tõusu sündmused ei tekitanud, kuid mõneks päevaks pöördus paljude inimeste tähelepanu materiaalselt väärtustelt teistele, samuti inimlikele.

## **Väljakutse teenuse pakujatele**

Rünnakule järgnesid FBI agentide külaskäigud paljude USA teenusepakujate juurde, et esitada hulk rutiinseid küsimusi. Ühe anonüümseks jääda soovinud Earthlinki töötaja sõnul tundsid agendid huvi konkreetsete aadresside ja isikute vastu.

Esialgu nõustusid koostööga nii Earthlink, America Online, Yahoo!, Microsoft, Excite@Home kui ka mitmed teised Interneti-ühendust pakuvad ettevõtted. EarthLinki asepresident sidealal Dan Greenfield kinnitas, et firma varustab riigi julgeolekuteenistusi teabega vaid ulatuses, milleks ta kohalike seaduste alusel kohustatud on.

Teine samm, mille USA võimud ette võtsid, oli küllaltki pealetükkiv ettepanek kohalikele teenusepakujatele: FBI esitas suurematele ISP-dele taotluse Carnivore'i jälgimissüsteemi rakendamiseks. Carnivore võeti laiemalt kasutusele möödunud aasta lõpus, et selle abil jälgida kuritegevuses kahtlustatavate isikute elektronposti. Carnivore'i kasutamiseks oli vajalik kohtu vastav order, mida tegelikkuses saab anda eeskätt konkreetse(te) isiku(te) kohta. Carnivore'i turuletulekut on algusest peale saatnud Ameerika inimõiguslaste küsimused ja kahtlused. Programmi kohta avaldatud valitsuse raportis kinnitati, et Carnivore ei riku privaatsust ega kodanikuõigusi, sest ei anna uurijaile rohkem infot, kui kohtuorder lubab.

Teenusepakujad lükkasid agentide ettepaneku valdavalt tagasi, kuid mitmed neist nõustusid oma serverites toimuvat jälgima oma tarkvara abil. Sellised otsused on kasutajates tekitanud hulga ärevust ja pahameelt, kuna paljudele tundub see isiklikesse asjadesse ninatoppimisena.

USA seadused on seni sätestanud luure- ja õiguskaitseorganitele, sh Föderaalsetele Juurdlusbüroole (FBI), Luure Keskagentuurile (CIA) ja eeskätt sõjaväeluurega tegelevale Rahvusliku Julgeoleku Nõukogule (NSA) kõikvõimaliku jälitustegevuse teostamiseks kindlad piirid.

Tegelikkuses on teatavad piirangud isikute privaatsusele siiski lubatavad eeldusel, et need on vajalikud näiteks riigi julgeoleku, ühiskondliku turvalisuse või riigi majandusliku heaolu huvides, korratuse või kuriteo ärahoidmiseks, tervise või kõlbluse või inimeste õiguste ja vabaduste kaitseks. Konkreetset eeldused tulevad reeglina siseriiklikust õigusest. Sama võimalus oleks täiesti olemas ka Eestis: põhiseaduse paragrahv 43 sätestab igapäev õiguse tema poolt või temale posti, telegraafi, telefoni või muul üldkasutataval teel edastatavate sõnumite saladusele, kuid võimaldab sellest erandeid kohtu loal kuriteo tõkestamiseks või kriminaalmenetluses tõe väljaselgitamiseks seadusega sätestatud juhtudel ja korras. Eesti on ühinenud ka Euroopa inimõiguste ja põhivabaduste kaitse konventsiooniga, mille artikkel 8 annab võimaluse sekkuda isiku korrespondentsi saladusse.

## **Meeleavaldused**

Pärast toimunut on e-kanaleid kasutatud oma emotsioonide ja arvamuste väljajätleamiseks. Katastroof vallandas Internetis kettkirjade laviini, mis on muide üks e-õiguses seni valdavalt tähelepanuta jäänud temaatika.

Üks tõsine e-õiguse alane üleastumine seondus otseselt Eestiga: vähem kui nädal pärast katastroofi süüdistas 16-aastane Ahtme koolipoiss Ameerika Ühendriikide presidenti 11. septembril Maailmakaubanduskeskuse ja Pentagonis vastu toime pandud

terrorirünnakutes ning ähvardas presidenti tappa. E-kirja laekumisest sai Eesti kaitsepolitsei teada Ameerika õiguskaitseorganeilt. Et õigusrikkuja ise on alaealine, on konkreetse teo tulemuseks halduskaristus poisil vanematele, kuid sarnaseid tegude toimepanijaid on erinevates riikides võimalik ka rangemalt karistada.

Ehk põhilise juurde: USA sündmuste järel sai uut kinnitust asjaolu, et nii mõnedki võtavad Interneti kui enda jaoks turvalist mängumaad, kus öeldu ja tehtu ei oma vähimaidki õiguslikke tagajärgi. Julgus, millest paljudel realses elus vajaka jääb, kasvab võrgus sageli lubatud piiridest ülegi.

Inimõiguste konventsiooni artikkel 10 sätestab küll isiku õiguse sõnavabadusele: see õigus kätkeb vabadust oma arvamusele ning vabadust saada ja levitada teavet ja mõtteid ilma võimude sekkumiseta ja sõltumata riigipiiridest. Kuna nende vabaduste kasutamisega kaasnevad kohustused ja vastutus, võidakse sõnavabadust seostada niisuguste formaalsuste, tingimuste, piirangute või karistustega, mis on fikseeritud seaduses ning on demokraatlikus ühiskonnas vajalikud riigi julgeoleku, territoriaalse terviklikkuse või ühiskondliku turvalisuse huvides, korratuste või kuritegude ärahoidmiseks, tervise või kõlbluse või kaasinimeste reputatsiooni või õiguste kaitseks, konfidentsiaalse teabe avalikustamise vältimiseks või õigusemõistmise autoriteedi ja erapooletuse säilitamiseks.

### **Ekspertide koondamine**

USA president George W. Bush moodustas kiire korras ekspertkomitee, mille ülesandeks sai assisteerida riigipead küberturvalisuse küsimustes. Bush andis korralduse moodustada küberterrorismi osakond ülesandega leida uusi mooduseid arvutivõrkude kaitsmiseks. Osakonda hakkab juhatama presidendi erinõunik küberturvalisuse küsimustes, Richard Clarke .

Kongressi terrorismivastase võitluse komitee eesistuja James Gilmore on teinud ettepaneku jätkata ka erinevate valitsusasutuste juurde moodustatud Y2K büroode tööd ning kujundada need ümber asutustekeskseteks küberturvabüroodeks.

Tulemuseks on ulatuslik rinne võrguturvalisuse kontrollimiseks ja tagamiseks. USA rünnakud Afganistanile on andnud ühendriikide valitsusasutustele põhjust olla valmis uuteks katsumusteks, mida kardetakse saabuvat ka Interneti kaudu.

Ekspertide koondamine ja nendevaheline koostöö on hoogustunud kogu maailmas, et tagada süsteemi turvaprobbleemide preventatsioon, juba tekkinud probleemide väljaselgitamine ja likvideerimine.

### **Seadusandlik spurt**

Üksteise järel valminud seadused Uniting and Strengthening America (USA) Act ja Provide Appropriate Tools Required to Intercept and Obstruct Terrorism (PATRIOT) Act sisaldavad piiranguid privaatsusele ning annavad võimudele õiguse sorida e-kirjade pealkirjades ilma seni nõutava kohtuorderita.

Euroopas ja mujalgi maailmas on töös või kavas olevad e-turvalisuse projektid uuesti päevakorda võetud. Täna seaks allakirjutamiseks avatud Euroopa küberkuritegude konventsiooni eesmärk on ära hoida arvutisüsteemide, võrkude ja andmete konfidentsiaalsuse, terviklikkuse ja kättesaadavuse vastu suunatud kuritegusid ja süsteemide väärkasutusi, mille saavutamiseks on konventsioonis kriminaliseeritud mitmed sellekohased teod.

Iseenesest on kogu õigusbaasi muutmine ja täiendamine suunatud efektiivsemale koostööle küberkuritegevuse (mille hulka kuulub vaieldamatult ka küberterrorism) tõkestamiseks ja kurjategijate väljaselgitamiseks ning karistamiseks. Tegude kriminaliseerimine on teisejärguline ülesanne, sest juba praegu võimaldab enamikes riikides kehtiv õigus küberkurjategijaid karistada. Probleemaatiline on riikide koostöö efektiivsus kriminaalmenetluse alal ning just see on seadusandjate jaoks praegu üks prioriteetvaldkondi.

Ka USA seadusandlikud sammud teenivad eelkõige riigis valitsevate emotsioonide ja erimeelsuste silumise eesmärki. Küsitlustulemuste kohaselt ei leia enam ameeriklasi, et vastuvõetud regulatsioon oleks tavapärasest palju erinev. Peamine iseärasus võrreldes tavaliste arengutega e-õiguses on praegune reguleerimiskiirus, mis seab vähemalt USA seadusandjate otsuse- ja analüüsivõime aukartustäratavale positsioonile.

### **Prioriteetide ülevaatamine**

FBI Arvutikuritegevuse osakond on hoiatanud kasvava küberprotesti ja häkkerluse eest seoses 11. septembri sündmustega. Arvatakse, et kuigi enamik sellisest tegevusest keskendub konkreetsetele saitide ja teenusepakujate ründamisele, tuleb senisest enam keskenduda rahvuslike infrastruktuuride küberturvalisuse tagamisele.

Mitmed USA juhtivpoliitikud on kinnitanud, et Ameerika küberruum vajab igakülgset kaitset olenemata sellest, kas võimalik rünnak langeb riistvarale, mis majutab märkimisväärset hulka rahvuslikust Interneti-pagasist või tarkvarale ja Interneti kontroll-mehhanismidele.

### **Infolekked kartus**

Paljud USA valitsusasutused kadusid küberkeskkonnast määramata ajaks. Tõsiasi, et nende füüsiline turvalisus on ohustatud, andis oma impulsi ka küberkeskkonna turvalisusele kriitilise pilguga vaadata. Eriti hoolikalt on Internetist maha võetud strateegiliselt tähtsat infot ja näiteks kõikvõimalikku tuumaalast teavet sisaldanud saidid.

### **Rünnak anonüümsusele**

Senisest enam on arutlusel ka anonüümsuse küsimused. USA-s pole seni kasutusele võetud ID-kaarti, kuid nüüd räägitakse ka võimalikust kohustusest end küberruumi sisenemisel nõ kirja panna. Kaasaegne ID-Kaart (see, mille kasutuselevõtmine on kõne all USA-s) ei ole lihtsalt plastikkaart, vaid interaktiivse tehnoloogia üks komponent, mis mängib masinavärgile kätte isiku kõige

delikaatsemad andmed.

ID-kaartide vastased on toonud välja uute isikuttõendavate dokumentide nõrgad kohad: kõnealuste kaartide kasutuselevõtmisega kaasneb kriitikute arvates kolm asjaolu, mis mõtlematu või lohaka käitumise tulemusena võivad isikute privaatsfääri oluliselt kahjustada: esiteks peab iga kodanik loovutama riiklikku andmebaasi oma sõrmejälje, mis seostatakse muude isiku kohta käivate andmetega (rass, vanus, kodakondsus ja foto).

Teiseks on valitsuse huvi kohustada isikuid ID-kaarti kasutama võimalikult paljudel asjaoludel ja paikades (bussis, lennujaamades, koolides, ujulates jne) ja ID-kaardi kasutuselevõtmega kasvaks ka politsei pädevusulatus. See tähendaks valitsusele muuhulgas ülevaadet isiku liikumistest ja asjaajamistest. Lisaks sellele võimaldab kaardisüsteem informatsioonivahetust kõigi valitsusasutuste vahel.

Just süsteemi üliturvalisus muudab selle iseendale ohtlikuks: praktika on seni näidanud, et ka kõige turvalisemaks peetud kaardid on varsti pärast avalikku tutvustust saadaval nõ blankettidena, mis võimaldab kurjategijatel ja terroristidel toimetada võltskaardi abil hoopis turvalisemalt ja vabamalt, kui erinevate senikehtinud isikuttõendavate dokumentidega.

## Lõpuks

Ei saagi väita, nagu oleks terrorirünnak e-õiguses midagi kardinaalselt muutnud. Samas on avalikkuse, ja mis veelgi olulisem, riikide valitsuste ja seadusandjate tähelepanu pöördunud e-turvalisuse küsimustele ning see loob soodsa pinnase võimalikeks edasisteks arenguteks.

### Artikkel 8 - Õigus austusele era- perekonnaelu vastu

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.

- [Lahendused](#)
- [Turvalisus](#)