Jäljerida digiaedikus

Kaido Kikkas

(Algselt avaldatud ajakirjas "30 pluss" mais 2016, siin ilmub kokkuleppel toimetusega)

Moto: "Kui räägitakse privaatsusest ja vastutusest, siis inimesed kipuvad nõudma enesele esimest ja teist nõuavad teistelt." - David Brin, ameerika teadlane ja ulmekirjanik

Paljude jaoks seostub Internet veel tänagi piiramatu vabadusega. See on koht, kus võib olla ükskõik kes - koll, loll või troll. Ja keegi ei saa ju teada, eks...?

Ent juba mõnda aega ei ole asi päris nii lihtne. Internetis on võimalik jälgi segada ja teadja inimene suudab end vähemalt mõnda aega ka üsna edukalt varjata, ent tavainimese reaalsus on see, mida USA meediauurija Mark Andrejevic on nimetanud digiaedikuks (*digital enclosure*) - iga võrgus tehtud samm jätab maha info sammu toimumise kohta ehk digitaalse jalajälje. See võib olla nii passiivne (infot kogutakse isiku tahtest sõltumatult - näiteks tema arvuti IP-aadress) kui ka aktiivne (isik ise nõustub mingi teenuse tarbimiseks enda andmeid edastama - näiteks Facebooki kontot luues).

Muide, ka kaht suurt internetiajastu lekkeskandaali - Wikileaksi ja hiljutist Panama paberite lugu - võib lugeda globaalse digiaediku loomulikuks osaks. Tõenäoliselt ei oleks Islandi ja Briti peaministrite rahamängud veel mõnekümne aasta eest kunagi meediasse jõudnud, nüüd aga tõid digijäljed kaasa tõsise pahanduse.

Tänapäeva nutiajastul ei piirdu jäljerida vaid arvutitega. Samamoodi käituvad nii nutitelefonid kui ka muud "targad seadmed" nagu nutitelerid. Ning sageli on piir mugavuse ja ahistamise vahel üsna õhuke - nagu oleme varem juba maininud, loobuvad paljud enda privaatsusest just nimelt mugavuse huvides.

Ja viimaks - digijäljed ei pea olema suured ja selged. Hea näide on kirjas Stanford Reporti eelmise aasta augustinumbris (https://news.stanford.edu/news/2015/august/social-media-kosinski-082515.html), kus Stanfordi kõrgema ärikooli organisatsioonikäitumise dotsent Michal Kosinski väidab, et inimese Facebooki "laikide" järgi saab otsustada, kas tema vanemad on abielus või lahutatud.

Jäljeajajad ja motiivid

Digitaalseid jalajälgi ajavad paljud ning neid on olemas terve skaala ulatuses. Toome mõned (NB! täiesti väljamõeldud, ent siiski üsna usutavad) näited:
* perearst uuris mu digitaalset haiguslugu (mis suuresti koosneb samuti meie digijälgedest, mille oleme jätnud erinevate arstide ja apteekrite arvutitesse) ja sai varajases staadiumis jälile ohtlikule haigusele. IT päästab elusid!
* mobiilioperaator saatis teate, et 20-aastase kliendistaaži täitumise puhul kingivad nad mulle kaks piletit suvel Tallinnas toimuvale Queeni ja Adam Lamberti kontserdile. Vau, uskumatu! Juhuu! Aga... Kust nad teavad, et olen Queeni fänn nende esimesest albumist saadik...?
* Google viskab mulle pidevalt ekraanile reklaame. Tüütu, aga vähemalt on seal teinekord üllatavalt asjalikke pakkumisi. Kuidas nad seda oskavad?
* Kapo kutsus mind kohvile. Njah, poleks pidanud ühe seltskonnaga foorumis bin Ladeni teemal nalja viskama...

* Hiljuti oli paras jama ühe Läti äripartneriga. Nendega võttis ühendust keegi tegelinski, kes suutis niivõrd detailselt "mina olla" (alates äriandmetest ja lõpetades kirjastiili ja naljadega), et lätlased saatsid vanale partnerile suure kaubapartii ära ilma maksekorralduse täitmist ära ootamata. Nüüd on kaup vasakul, lätlased nördinud ja raha pole kusagil.

Nagu näeme, on tegu väga erineva lõpuga lugudega, kuid ühine on üks - kõigis on kesksel kohal detailse info kogumine inimese kohta, erineb vaid selle info kasutamine. Esimene on nii loomulik, et keegi ei kipugi siin mingit probleemi nägema (välja arvatud ehk info sattumine valedesse kätesse). Teine on hea näide Interneti toimikuefektist - firma on andnud järele kiusatusele koguda kliendisuhtest märksa laiemaid andmeid ning Queeni piletid seda ei kompenseeri. Kolmas esitab firmat, kelle jaoks info ongi äriobjekt. Neljas on näide Suure Venna stsenaariumist ning viimane on juba klassikaline sotsiaalmanipulatsioon, kus väljapetetud info viis kuriteoni.

Mida siis teha?

Eestis oli kunagi üks minister, kes läks ajalukku soovitusega "ära topi sinna, kuhu pole vaja". Internetis on see soovitus täiesti asjakohane - eeskätt just aktiivsete digijälgede osas (e-postiaadress, kasutaja- ja pärisnimed, elukohaandmed, aga tänapäeval kohati ka näiteks FB kontoinfo ja muud küberruumi kohanäidikud). Seega esmane soovitus on "enne mõtle, siis sisesta". Lisaks sellele aga võib anda veel mõned ideed.

Passiivse digijälje vähendamiseks:

* vaata üle nii operatsioonisüsteemi, veebilehitseja kui konkreetse rakenduse sätted - näiteks FB-st oleme juba rääkinud, veebilehitseja turvamine tuleb aga eraldi teemana vaatluse alla tulevikus.
* kasuta veebilehitseja privaatrežiimi (mida irvhambad "pornorežiimiks" kutsuvad) - Chrome ja Chromium nimetavad seda *incognito*-režiimiks (Ctrl-Shift-N), Firefox privaataknaks (Ctrl-N), Safari puhul avaneb see menüüst (kuid sinna saab ka kiirklahvi defineerida). Selle tulemusena ei salvestata sirvimise ajalugu, otsinguid ega mitmeid muid asju.
* Kaug- ja kodustöötajad teavad ilmselt juba, mida tähendab VPN ehk virtuaalne privaatvõrk. Neid on võimalik kasutada aga ka mujal kui vaid tööandja võrku ühendumisel - näiteks https://www.hidemyass.com/ või https://www.your-freedom.net/. Lisaks võib vaadata näiteks aadressilt http://proxy.org/.
* Kasuta jälgimist vähendavaid ja sellest teavitavaid teenuseid nagu Privacy Badger: https://www.eff.org/privacybadger
* Igapäevaste veebiotsingute jaoks võiks kasutada Google'i otsingumootori asemel näiteks DuckDuckGo'd (https://duckduckgo.com/; mitmed Linuxi distrod kasutavad seda juba mõnda aega).
* Tõsisema jäljesegamise jaoks kasuta Tor'i: https://www.torproject.org/projects/torbrowser.html.en (ka sellest räägime edaspidi lähemalt).
* Kasuta erinevate teenuste jaoks erinevaid kontosid - mida rohkem erinevaid jälgi, seda raskem on jäljeajajal suurt pilti kokku panna.
* Väldi võimaluse korral integreeritud teenuseid - näiteks sisselogimist Google'i või FB kontoga.
* Google võimaldab (teatud määral) infot kustutada. Lähemalt võib vaadata veebist: https://support.google.com/accounts/answer/465?hl=et.
* Tasub kaaluda elementaarse Linuxi kasutusoskuse omandamist (sellestki on plaanis lähiajal lähemalt rääkida). Enamik tänaseid Linuxeid suudavad käivituda mälupulgalt ning jätta kõvaketta puutumata - see on väga hea viis lühiajalise, ent privaatsust nõudva veebisirvimise jaoks.
* Mobiilseadmetel tasub võrguühendus käivitada vaid selle kasutamise ajal - enamasti saab selle käivitamiseks mugavalt otse avaekraanilt kasutada erinevaid vidinaid. Veelgi enam, kui kasutame tundmatumat sorti äppe (eriti mängud ja muu ajaviide), siis oleks soovitus teha seda lennukirežiimis - nii ei saa äpp meie selja taga sigatseda.

* Tasub kindlasti üle vaadata, milliseid õigusi taotlevad paigaldatavad mobiiliäpid. Kas see lõbus ahvimäng tõesti vajab ligipääsu minu kontaktinimekirjale...?
* Võiks ka lisada (mõne jaoks lausa ketserliku) soovituse osta endale vana kooli tavamobla. See ei pea olema tingimata ainus (või isegi peamine) sidevahend, aga näiteks suvel maale puhkama sõites võiks olla päris hea idee tõsta SIM-kaart sinna ja piirduda kuu aega vaid hädapäraste kõnedega.

Aktiivse digijälje vähendamiseks:

* kustuta ära vanad kasutajakontod, mida enam ei vaja - see aitab ära hoida identiteedivargusi ja teatud määral vähendab ka jälge. Siiski tuleb arvestada, et info säilib tõenäoliselt nii kohalikes arhiivides kui veebipõhise teenuse puhul sageli ka Interneti Arhiivis (archive.org). Samuti võivad mõned teenused konto vaid välja lülitada (mitte kustutada andmeid), mõni teenus võib aga lubatud kustutamise lihtsalt täitmata jätta.
* vaata üle igasugused listid ja kampaaniakohad (eriti Facebookis) ning kus vajalik ja võimalik, proovi end eemaldada. Siin tasub viidata varasemale Google-Fu teemale - see võimaldab iseennast otsida eri paigust ning kui me ei mäletagi, et end kahe aasta eest kuhugi listi panime, siis tasub end sealt kindlasti maha võtta.
* tee endale äravisatav e-postiaadress, mida kasutad üksnes erinevatesse teenustesse registreerumiseks (mõnel juhul on kasutamahakkamiseks vaja ka teenusepakkuja kirja vastuvõtmist). Ühekordsete (ja kahtlasema väärtusega) sisselogimiste jaoks tasub kasutada teenuseid nagu näiteks 10minutemail.com - samas peab jälgima, et need omakorda ohutud oleksid.
* veel kord - mõtle hoolikalt läbi, mida kirjutad, mida üles laed, mida jagad ja mida "laigid". Üks veebis laialt levinud seletus pilveteenuse kohta on "poliitiliselt korrektne sõna, mis tähendab kellegi teise arvutit"...

Lõpetuseks

Edasiseks lugemiseks soovitaks seekord Tony Fishi raamatut "My Digital Footprint: A two-sided digital business model where your privacy will be someone else's business!", Mark Andrejevici "iSpy: Surveillance and Power in the Interactive Era" ning Kieron O'Hara ja Nigel Shadbolti "The Spy in the Coffee Machine: The End of Privacy As We Know It" (sel teemal on tegelikult häid kirjutisi päris palju). Põhiline on aga (nagu paljude muude teemade juures) ports ettevaatust ning tervet talupojamõistust.