Kuidas ajakohastada Eesti digiidentiteeti?

Eesti on e-riigi ekspordil olnud üliedukas. Mõnikord me üllatume, et miks teised riigid pole läinud täpselt sama teed. Mis neid takistab? Vahel on põhjuseks meie väiksus ja võimekus riske võtta. Hoopis sagedamini aga põhjustavad loidu toimimist teatud kultuurilised hoiakud ning salahirmud, mida me Eestis isegi ei tunneta – näiteks on Euroopa privaatsustraditsioon oluliselt sügavamate ajalooliste allhoovustega.

Kui jutt käib arengust, siis mis suunas peaks Eesti edasi liikuma? Kas meie isikukoodi kuju võib häirida Euroopa privaatsustraditsiooni? Sisaldab see ju sugu ja sünnipäeva (ning mõne põlvkonna puhul väljendab varjatult isegi sünnikohta). Kas me peaksime oma isikukoodis mõned andmed hägustama, nagu Läti juba tegi ja Soome varsti teeb? Kui revolutsioonilised peaksime olema? Kas piisab ühest eluaegsest isikukoodist või peaks kodanikule väljastama terve elu jagu plokiahelal põhinevaid äraantavaid isikukoode? Nüüd räägime sellest kõigest põhjalikumalt.

Identiteet

Oma esmase identiteedi saab inimene DNA kujul oma bioloogilistelt vanematelt. Igas enesest lugupidavas riigis on vähemalt üks DNA-labor, mis võimaldab riigi käes olevat jõumonopoli kasutada ning tuvastada avaliku korra aluseks oleva objektiivse tõe: et isik on olnud otseses puutumuses eseme või kohaga.

Eesti digiriigis on mindud üks samm edasi. Digimaailm ei ole seni looduse antud võimalusi kasutanud, vaid seab iga indiviidi juriidilisse vastavusse bitikujulise identiteediga. Digimaailma loogika on ümber pööratud: puutumust ei uurita pärast ja laboris, vaid inimene pannakse identiteedi (ja selle kandjate) väljastamisega olukorda, kus tal ei õnnestu õieti ühtki elukondlikku toimingut sooritada ilma endast digijälge jätmata. Digiallkiri polegi tegelikult muud kui isiku tõsikindel sidumine dokumendi ja ajaga.

Võiks arvata, et Eesti kodaniku identiteet peitub sertifikaatides, mis SK ID Solutions (1) (või mõni nende konkurent) ID-kaardile paigutab ning mille PPA isikule väljastab. Ent tõde on sügavamal. Eesti kodaniku (ja residendi) tegelik identiteet asub piltlikult öeldes hoopis politseiameti keldris – serveris ja andmebaasis. Siit tuleneb baas- ehk alusidentiteedi mõiste: alusidentiteet tekib teadaolevate vanemate järeltulijat registreerides, mõnel juhul aga ametniku tahtliku otsusega pärast isikut tõendavate dokumentide hindamist või pärast sõrmejälgede või silmaiirise kohustuslikku salvestamist. Kokku võttes: ID-kaart talitleb vaid identiteedi ajutise kandjana (nt tähtajaga 3 või 5 aastat).

ID-kaarti (ja selle teisendeid, nt elamisloa- või e-residendi kaarti) saab välja anda üksnes isikule, kelle alusidentiteet on PPA üliturvatud andmebaasis juba olemas. Ajakirjandus on käsitlenud näiteks nn Maarika/Ljuba juhtumit (2), kus süsteemis töötav isik korraldas just alusidentiteetide, mitte ajutiste identiteedikandjate võltsimist.

Nummerdamine

Andmebaasi administraator teab, et inimeste, objektide ja asjade omavahel segiajamise vältimiseks tuleb need kindlasti nummerdada: anda neist igaühele oma unikaalne ID-number (UID). Eesti inimestel on sääraseks numbriks isikukood. Ehk nagu ütleb Taavi Kotka: “Sinu digitaalne nimi.”

Isikukood on filosoofiliselt põnev teema. Taani hakkas residente arvele võtma juba aastal 1924 (3) ning aastast 1968 peetakse elanike registrit elektrooniliselt. Euroopas on isikute nummerdamisega siiski seotud ka mõnin-

gad kahtlused ja kõhklused, mis tulenevad asjaolust, et II maailmasõja ajal toime pandud koletud kuriteod said võimalikuks tänu kõigi elanike identifitseerimisele ning täpsele arvestusele (4). Kuivõrd koonduslaagrites kaotasid inimesed nime ja kandsid numbrit, siis selle raske ühiskondliku trauma mõjul välditakse isikute nummerdamist näiteks Saksamaal (5).

Samas pole raske mõista, et näiteks majanduslik kuritarvitus tekib pigem just siis, kui täpne arvepidamine puudub. Ükski piisaval arengutasemel digiriik ei saaks hakkama ilma alusidentiteedi mõisteta ega ka selle juurde käiva iga üksikut inimest üheselt identifitseeriva numbrita. UID alusel keskses andmebaasist suvalisi päringuid teha on liiga lihtne, mistõttu tekib uus küsimus: kes kontrollib kontrollijaid?

Just sel põhjusel laitis Euroopa Nõukogu eksperdigrupp naiivse numbrilise isikukoodi maha samal aastal, kui see Eestis kasutusele võeti – 1989. aastal (6). Ungari ülemkohus nurjas (7) isikukoodi kasutuselevõtmise katse just põhjusel, et see avanuks tee kontrollimatutele päringutele, millest ei jää ühtegi jälge. See võib olla üllatav, kuid eksperdigrupi poolt isikukoodidele ette heidetav kontrollimatute päringute risk on X-tee kontrollimehhanismide abil (Andmejälgija (8)) Eestis vägagi edukalt lahendatud. Andmesubjektil on võimalik vaadata, kes ja miks tema andmeid vaatas.

Ülalmainitud tabude tõttu nummerdatakse isikuid mujal Euroopas mõnevõrra varjatult, näiteks maksukohustuse kaudu, või lokaalselt riigi igal liidumaal ning ehk ka eriteenistuste andmefailides. Riigiülesest isikukoodist pole aga kusagil mujal peale Eesti kujunenud eredat sümbolit. Samas annavad just unikaalne nummerdamine ja sellele tuginev digitaalne identiteet e-riigis ärisuhetele täiesti uue mõõtme.

Avalik või salajane?

Eesti on selles küsimuses valinud naiivselt sirgjoonelise tee: isikukoodid on meil olemas ja avalikud. Teistes riikides see nii pole, näiteks USAs pruugitav SSN (Social Security number) on oma algmõtte järgi salajane. Paraku saab isikule omistatud salajane unikaalne number lekkida.

Omapärane probleem seondub andmebaasidega. Nimelt, riiklike registrite ülesehitus (disain) oleneb suuresti sellest, kas päringuid sooritatakse, tuginedes avalikule või salajasele identifikaatorile. Kui isikukood on kõigile teada ning selle paroolina kasutamine on otseselt keelatud, siis ei anna võõra isikukoodi nimetamine arusaadavalt kellelegi eelist. Andmebaasist ei tule pelga nimetamise peale ühtki lisabitti enne, kui küsiv isik on end tõsikindlalt identifitseerinud (näiteks ID-kaardiga) ning ta suudab näidata päringu

tegemiseks nõutavaid volitusi.

Parooli tüüpi isikukoodi puhul (nagu SSN) seevastu eeldatakse, et kui isik juba seda salajast numbrit teab, on ta ilmselt kuidagi õigustatud ka selle numbriga seotud andmeid küsima. Tagajärg: mitme riigi väga tähtsates andmebaasides ei üritatagi päringu tegijat identifitseerida, samuti ei jää ainsatki jälge sellest, kes päringu tegi. Võõra isiku salajast koodi teades saab kätte ka andmed. Just see on põhjus, miks neis riikides on suuremahulised isikuandmete lekked väga levinud ja ühtlasi eriti ohtlikud.

Olen seda küsimust arutanud Belgia poliitiku Philippe de Backeriga, kelle hinnangul eeldab Belgia infosüsteemide üleviimine parooli tüüpi isikukoodilt avalikule, digitaalse nime tüüpi isikukoodile ei enamat ega vähemat kui riigi baasregistrite ümberdisaini maksumusega vähemalt kümneid miljoneid eurosid. Kokku võttes: Eestil on vedanud, sest tundub, et meie infosüsteemid on õigesti konstrueeritud.

Mitteunikaalse identiteedi murega põrkub Eesti aga juba 29. septembril 2018: päeval, kui eIDASe määrus (9) laieneb ka sisselogimisele (autentimisele) ning Eesti riigil tuleb oma portaalidesse sisse lubada Euroopa Liidu kodanikke riikidest, kus unikaalset nummerdust pidevalt eitatakse. Näiteks kui sakslane Max Mustermann kolib Baierist Hamburgi, väljastatakse talle täiesti uus digitaalne identiteet, sest Saksamaal on identiteet liidumaapõhine, mitte riigipõhine. Huvitav probleem: mille põhjal saaksid Eesti infosüsteemid järeldada, et tegu on sama isikuga?

Eesti isikukoodi ajaloo allhoovused

Tõenäoliselt suureneb lähiajal surve ajakohastada Eesti isikukoodi kuju.

Isikukoodi kasutuselevõtmise juurtest on arusaadavatel põhjustel vähe räägitud. Nimelt võeti isikukood meile üle 1989. aasta sügisel Moskvast, selle arvutamise valemi sõnastas Statistika Keskvalitsus standardis ENSV VST 585-89 ning see juurutati ENSV Plaanikomitee 1989. aasta 12. oktoobri määrusega nr 121.

Valemi aluseks olev arvutuskäik pärineb Ungarist ja selles sisaldub pisuke viga. Nii näiteks, kui kontrollida veebis vaid ühe numbri võrra erinevaid isikukoode 51107121760 ja 61107121760, siis kontrollsumma põhjal tunnistatakse mõlemad õigeks (10). Tegelikult peaks isikukoodi mingi numbrikoha muutudes vältimata muutuma ka kontrolljärk (siin näites viimane number “0”).

Varem, kui isikukoode dikteeriti telefonis, oli (toimiv) kontrolljärk kindlasti vajalik. Tänapäeval loetakse isikukoodi elektrooniliselt – ID-kaardilt – seega ei teki vigasest arvutuskäigust ülearu palju pahandusi. Inetuid lugusid selle vea tõttu siiski juhtub. Ajalehepealkirjad kajastavad neid umbes sedasi: "E-põrgu kadalipp: kuidas tõestada, et sa pole skisofreeniahaige?" (11).

Viga kontrollkoodi arvutamisel on mugav käsitleda põhjusena, mis sunnib meid isikukoodi reformima. Tegelikult on hoopis suurem see teine mure: Euroopa Liidu mõneti kultuurimarksistliku privaatsusparadigma raames ei ole isikukoodis sobilik noteerida ei sugu ega sünnipäeva.

Eesti rahvaarv on väike. Me tunneme niikuinii kõiki, me mäletame, millal nad sündisid ja mis soost nad on. Mitte ilmaasjata ei saadeta tunnistajakaitse kaitsealuseid Eestist mõnesse välisriiki (12).

Läti korraldas hiljuti isikukoodireformi (13) ja Soomel on see värskelt plaanis (14). Euroopa Liitu kuulumine tähendab, et Eestigi peab uuenduse ette võtma. Küll võiks Eesti hoiduda naiivsetest katsetest isikukoodi juhuslikustada pelgalt Euroopa Liidu rahuldamiseks. Kui muutused on vältimatud, peaks ehk Eesti teoks tegema hoopis Rahandusministeeriumi asekantsleri Dmitri Jegorovi ja teiste modernse idee (15), mille kohaselt kasutataks *estcoin*'i matemaatilisi algoritme isikule suure hulga juhuslike isikukoodide reserveerimiseks. *Estcoin* kõlab nii, nagu oleks tegemist bitirahaga, ent tegelikult tähendab see seda, et suur hulk juhuslikult genereeritud tingelemente (nn tõukeneid – ingl *token*) seotaks omavahel plokiahelasse ja neid saaks kasutada ühekordsete äraantavate isikukoodidena.

Nii säiliks kodanikul privaatsus Euroopa Liidu ranges tähenduses: keegi ei suudaks isikukoodi kuju järgi otsustada, kas tegu on Mardiga või hoopis naabri koeraga, kuid ühtlasi saaks kodanik igale andmenõudjale väljastada erineva (kuigi matemaatiliselt alusidentiteedile taandatava) isikukoodi. Säärane modernne isikukood on nii-öelda lekkimiskindel ja neid suurandmebaasidesse koguda oleks sama mõttetu kui kollektsioneerida liiklusmüra. Sel moel saaks Eesti oma (tegelikult Euroopa Liidu) "privaatsusprobleemid" lahendada e-riigile kohaselt – tulevikku vaataval ja teedrajaval moel. Mine tea, ehk saaksime seda lahendust eksportidagi.

Krediitkaardist

Küsime retooriliselt: kas ID-kaardi ja krediitkaardi vahel on ka muid sarnasusi peale alustehnoloogiate (kiip, plastik)?

Sarnasus on olemas ja küllaltki põhimõtteline. USAs ID-kaarti pole, küll aga on sealgi vajadus isikuid tõsikindlalt identifitseerida. Näib, nagu kuuluks krediitkaart jäägitult pangandusse ja tegeleks vaid võla teenindamisega, kuid ometi on USAs parema võimaluse puudumise tõttu krediitkaardile suudetud juurde pookida ka isiku tuvastamise funktsioon. Kui süveneda, siis võla teenindamiseks ongi isiku tuvastamine mööda¬pääsmatu. Ühendriigid tuginevad seega erafirmade pakutavale kaubanduslikule identiteedile, mille puhul tuleb isiku tuvastamise võimalus kaasa mitte otsese eesmärgi, vaid kaudse lisafunktsionaalsusena, vastandina Euroopale, kus identiteet kipub olema pigem riiklik.

USAsse viisavabal sisenemisel on krediitkaart suisa kohustuslik, ühtlasi ei õnnestu ilma selleta end USA hotellis sisse registreerida. Kas märkasite teatavat sarnasust meie ID-kaardiga? Erinevalt Eestist on USAs krediitkaartidel ülitugev seaduslik kaitse, mis ületab deebetkaardi oma mäekõrguselt (16).

Krediitkaart töötati välja 1940-ndatel (17), kui avalik sektor arvuteid veel ei kasutanud – oma aja kohta oli kindlasti tegu väga eesrindliku süsteemiga. Ent kuidas on lood praegu, kui enamik läänemaailma identiteedivargusi on paraku seotud just krediitkaartidega?

Aeg on vahepeal edasi läinud. Turvaline riiklik alusidentiteet vähendab oluliselt riski, et kurjategijat lahutab sinu varast vaid poolavalik kaardinumber ja kolmekohaline salakood (CVE2). Eesti on arenenud maailmale ette näidanud uutmoodi tee, kus inimestel puudub vajadus ühendada isikuandmed isiku rahalise seisuga (võimaldagu krediitkaart seda pealegi). Tänapäeva tehnoloogia¬maailmas, kus isik on ID-kaardi abil e-tuvastatud, pole ju probleemi talle pakkuda ükskõik missugust pangateenust (ka krediiti) Interneti vahendusel.

Eestist vaadatuna on krediitkaardi näol pigem tegu ajast mahajäänud Interneti-eelse tehnoloogiaga, mille riskid toob Internet eredalt välja. Sestap tuleb meil oma sõpradele ja liitlastele selgitada, et meil on pakkuda midagi hoopis uut ja põhimõttelisemat.

Anto Veldre
Infoturbeekspert

Kasutatud allikad

1. SK ID Solution www.sk.ee
2. Õhtuleht www.ohtuleht.ee/808101/dokumendivabrikant-tadi-ljuba-see-suudistus-on-uks-suur-vale
3. Scandinavian Journal of Public Health http://journals.sagepub.com/doi/pdf/10.1177/1403494810387965
4. Huffpost www.huffingtonpost.com/edwin-black/ibm-holocaust_b_1301691.html
5. Wikipedia (saksa keel) https://de.wikipedia.org/wiki/Volksz%C3%A4hlungsurteil
6. Council of Europe https://rm.coe.int/16806845b3
7. Privacy International https://web.archive.org/web/20110120075253/http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-64762
8. Geenius https://geenius.ee/uudis/riigiportaali-andmejalgijast-naeb-seda-kes-su-isikuandmeid-on-parinud
9. Majandus- ja kommunikatsiooniministeerium https://www.mkm.ee/sites/default/files/dhn_2016_02_17_eidas.pdf
10. Arvud https://arvud.com/et/kalkulaator/isikukoodi-test
11. Eesti Päevaleht http://epl.delfi.ee/news/eesti/e-porgu-kadalipp-kuidas-toestada-et-sa-pole-skisofreeniahaige?id=77783596
12. Eesti Päevaleht http://epl.delfi.ee/news/eesti/tunnistajakaitse-annab-uue-elu?id=50993272
13. Postimees https://maailm.postimees.ee/4166321/lati-loobub-isikukoodides-sunniaja-markimisest
14. Postimees https://www.postimees.ee/4272891/soome-hakkab-isikukoode-muutma
15. Geenius https://geenius.ee/uudis/restart-mis-estcoini-idee-ja-mida-see-tegelikult-tahendab
16. Wikipedia https://en.wikipedia.org/wiki/Credit_CARD_Act_of_2009
17. Credit Card https://www.creditcards.com/credit-card-news/history-of-credit-cards.php