Maire Iro - AKI

Teema: FW: Päring - Geeniuse/DelfiTV eksperiment

From: Maire Iro - AKI
Sent: Thursday, May 7, 2026 9:10 AM
To: 'Ronald Liive' <ronald.liive@geenius.ee>
Cc: press - AKI <press@aki.ee>
Subject: RE: Päring - Geeniuse/DelfiTV eksperiment

Tere, Ronald!

Aitäh väga põneva ja andmekaitse vaates paljude jaoks ilmselt silmiavava eksperimendi eest!

> See eksperiment kirjeldab tegelikult väga hästi tänast reaalsust. Peamine probleem ei ole üksikute andmete avalikkuses. Isegi kui iga infokild eraldi vaadates tundub tühine, siis neid kokku pannes tekib inimesest üllatavalt detailne pilt. Just see erinevatest allikatest pärit andmete sidumine suuremaks tervikuks ongi digikeskkonnas väga suur risk. Sel moel on võimalik inimest üsna üksikasjalikult profileerida.
>
> Tervikpilti vaadates ei piisa ainult küsimusest, kas mingi konkreetne info on seaduse järgi avalik või mitte. Avalikke andmeid peab vaatama tervikliku kogumina, et selliseid profileerimise riske maandada. Sealt edasi tuleb küsida, millised andmed siis avalikult kättesaadavad peavad olema ja millised mitte. Vajadusel tuleb varasemad otsused andmete avalikkuse osas ümber hinnata ja seaduse tasandil teisiti reguleerida.
>
> Lisaks peab ka avalikult kättesaadavate andmete puhul läbi mõtlema, milliseid kaitsemeetmeid kasutada, näiteks kas päringu tegemine nõuab autentimist ja kas sellest jääb maha jälg.
>
> Pensionisammaste liitumise kontroll on siin hea näide. Inimene peab oma pensioniandmete nägemiseks sisse logima, aga samal ajal saab võõras isik üksnes isikukoodi teades kontrollida liitumist ilma autentimiseta. See ei ole tervikuna tasakaalus lahendus. Avalikkus ei välista täiendavaid kaitsekihte nagu autentimine või logimine.
>
> Sama loogika kehtib ka teiste teenuste puhul, millest juttu oli. Küsimus ei ole ainult selles, kas see info peab olema kättesaadav. Siin tuleb lisaks mängu ka läbipaistvuse küsimus. Kas inimene saab hiljem aru, kes ja millal tema kohta päringuid tegi?
>
> Seadusandjal tuleb siin vaadata kahte asja korraga. Esiteks, millised andmed peaksid üldse olema nii lihtsalt avalikult kättesaadavad olukorras, kus neid on väga lihtne muude andmetega kokku viia. Ja teiseks, kui andmed on avalikud, siis millised tehnilised lahendused tasakaalustavad seda avatust. Autentimine ja päringute logimine ei ole erandlikud meetmed, vaid peaksid olema tavapärane praktika.
>
> Siin on oluline samm edasi ka andmejälgija, mis annab inimestele ülevaate, kes nende andmeid avalikes registrites vaatab. See ei piira päringute tegemist, kuid muudab need läbipaistvamaks. See omakorda distsiplineerib ka neid, kes muidu võiksid vaadata andmeid pahatahtlikult, omakasu eesmärgil või ka lihtsalt uudishimust.
>
> Isikukoodi puhul tasub selgitada, et eraldiseisvana ei ole see nii tundlik info, kui sageli arvatakse. Isikukood on isikuandmete vaates oma olemuselt võrreldav inimese nimega. Samas on see unikaalne tunnus, mille teadmine teeb erinevatest allikatest pärit andmete kokku sidumise ja

profileerimise väga lihtsaks. Risk peitubki pigem selles, kui palju infot on võimalik isikukoodi teades kokku panna.

Lisaks riigi ja asutuste vastutusele on oluline ka inimeste enda teadlikkus. Igal inimesel tasub aeg-ajalt vaadata, milliseid andmeid tema kohta internetist leiab. Samuti teadlikult läbi mõelda, millist infot ta ise näiteks sotsiaalmeedias või erinevatel veebiplatvormidel jagab. Mida teadlikum inimene oma andmete kättesaadavusest on, seda väiksem on tõenäosus, et tema andmeid kasutatakse pahatahtlikult, ning seda paremini oskab ta ka võimalikke riske ennetada.

Loodan, et neist mõtetest on jätkuloo kirjutamisel abi. Kui tekkis lisaküsimusi, siis võid alati uuesti ühendust võtta.

Heade soovidega

Maire Iro
Avalike suhete nõunik
maire.iro@aki.ee
5385 4644, 627 4136

ERAELU KAITSE JA RIIGI LÄBIPAISTVUSE EEST
Tatari 39 | 10134 Tallinn | Eesti
LinkedIn | YouTube

ANDMEKAITSE INSPEKTSIOON