

36. EESTI
ÕIGUSTEADLASTE
PÄEVAD

PÕHISEADUS | ∞

Andmekaitse „sõjaajal“ ja „rahuajal“ kroonviiruse kriisis

Dan Bogdanov, PhD

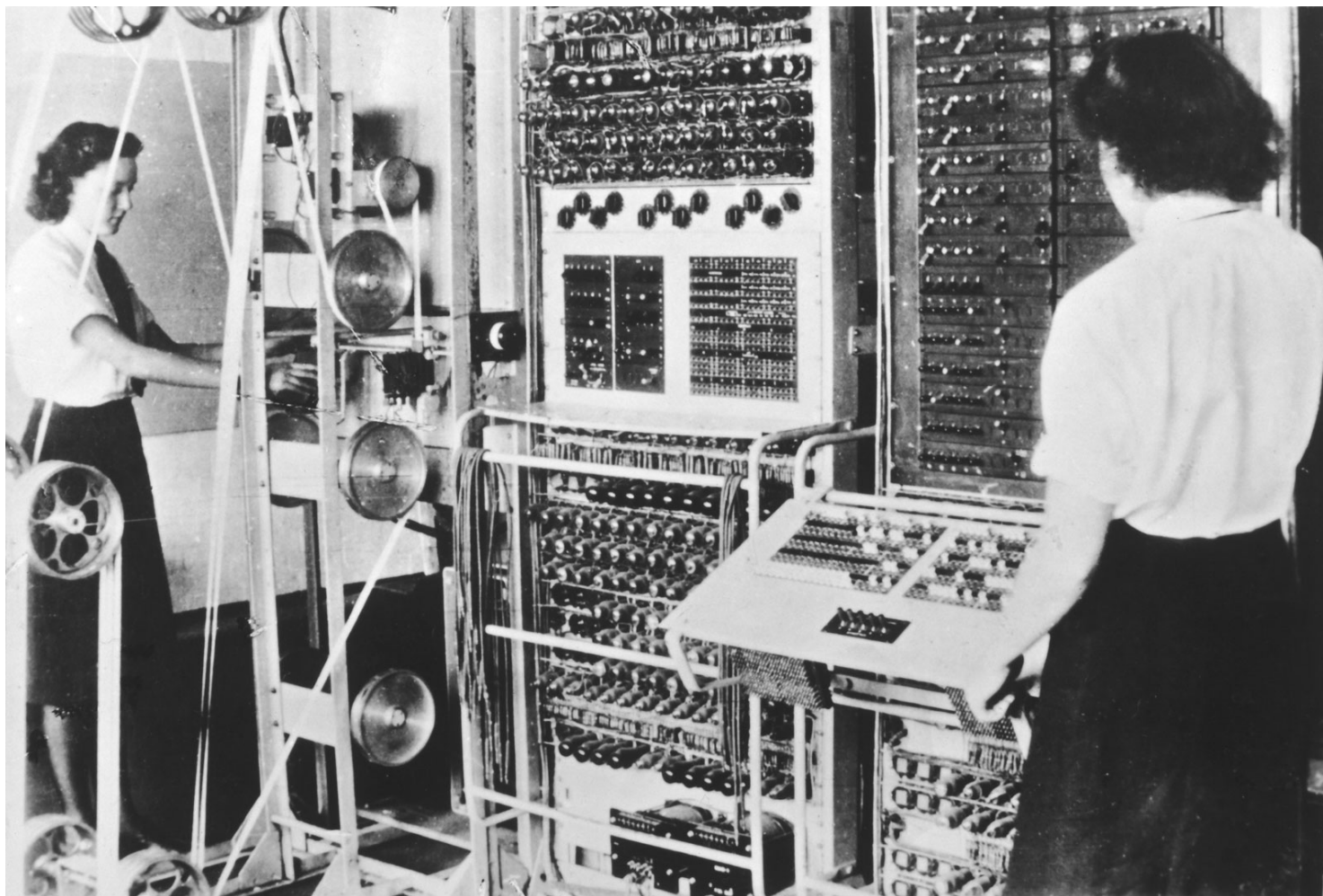
Cybernetica AS infoturbesüsteemide osakonna juhataja

Ettekande koostamisel on toetunud artiklile:

Dan Bogdanov, Triin Siil. Infotehnoloogilised võimalused põhiõiguste kaitsel. Juridica, 2020.

Andmekaitse “sõjaajal”

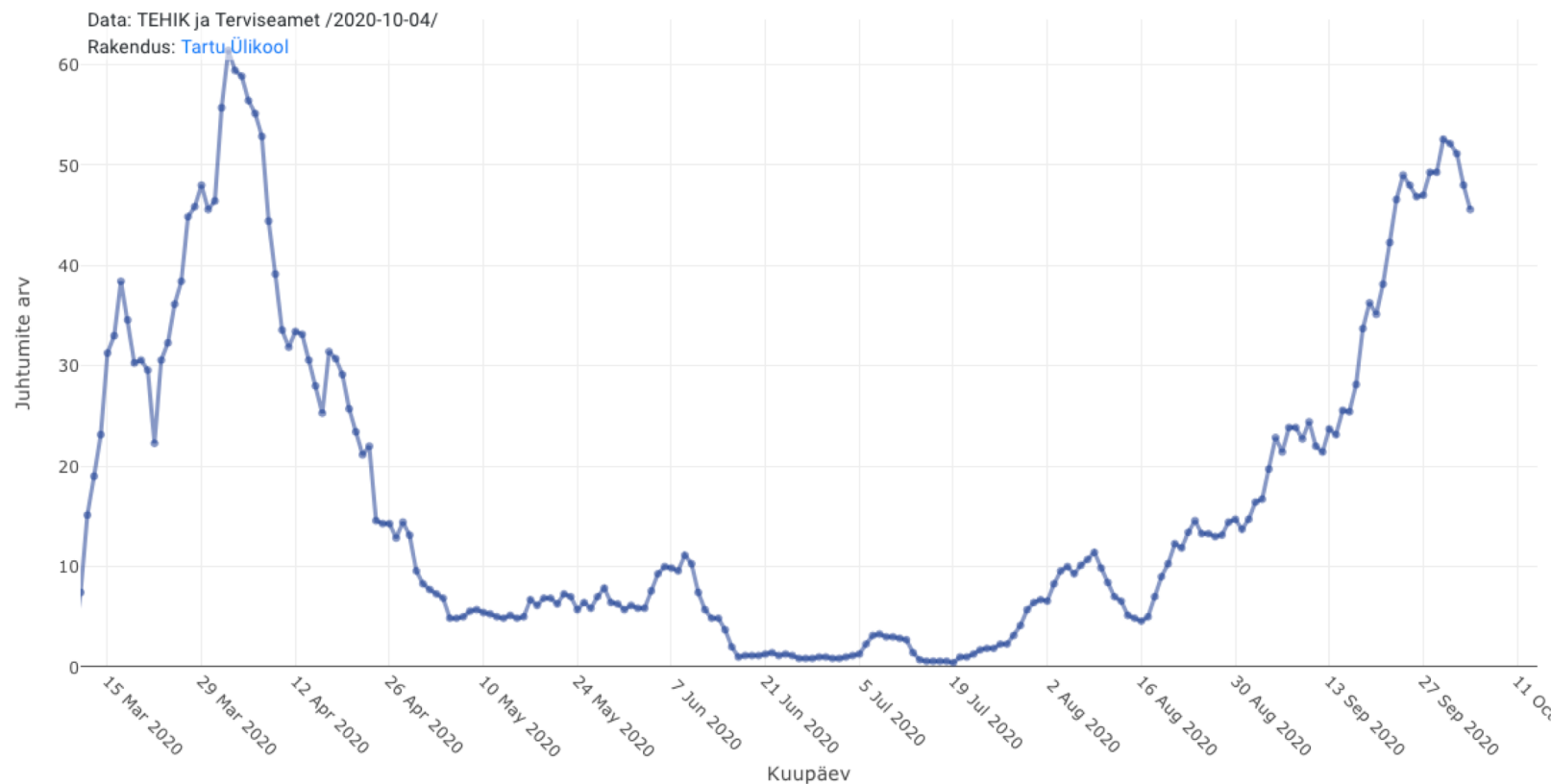
Mis tõi meid tänase andmekaitseni?



- **Colossus** (1943) oli esimene digitaalne elektronarvuti.
- See ehitati Inglismaal Saksa Lorenz SZ salakirjaseadme murdmiseks.
- Turvalisust on arvutitele alles hiljem hakatud juurde ehitama.

Foto allikas: *The History Blog*. <http://www.thehistoryblog.com/archives/21186>

SARS-CoV-2 viiruse kriis



- SARS-CoV-2 viirus on kiire levikuga kroonviirus, mis hakkas Eestis levima 2020. aasta alguses.
- Teadmatus ja hirm tõid tervisekriisi ja erakorralised tõkestusmeetmed.

Eesti positiivsete SARS-CoV-2 testide arv päevas, 7 päeva keskmine (märts-oktoober)
Graafiku allikas: Tartu Ülikooli töövahend <https://koroona.ut.ee>

Andmetega kriisi vastu

36. EESTI
ÕIGUSTEADLASTE
PÄEVAD

PÕHISEADUS | ∞

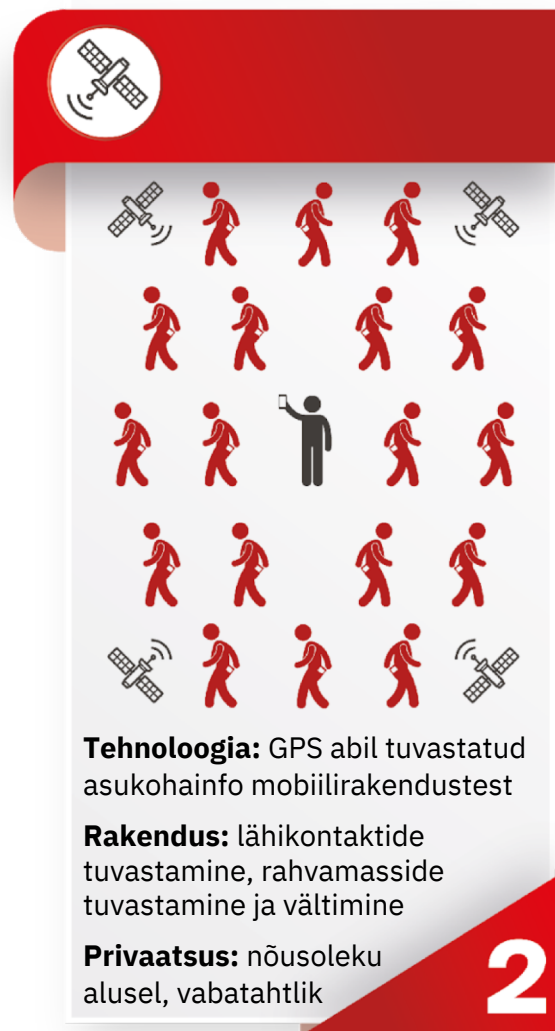


Tehnoloogia: inimeste liikumist jälgitakse mobiilimastide vahel trianguleerimise teel, andmed tulevad mobiilioperaatoritelt

Rakendus: piirangute kontroll

Privaatsus: nõusolekuta, kogu populatsioon

1

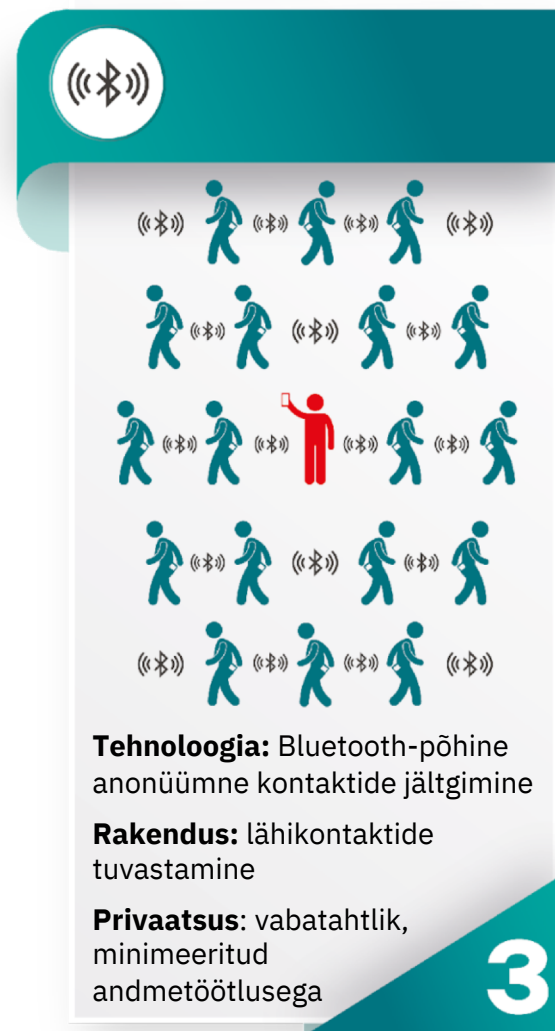


Tehnoloogia: GPS abil tuvastatud asukohainfo mobiilirakendustest

Rakendus: lähikontaktide tuvastamine, rahvamasside tuvastamine ja vältimine

Privaatsus: nõusoleku alusel, vabatahtlik

2



Tehnoloogia: Bluetooth-põhine anonüümne kontaktide jälgimine

Rakendus: lähikontaktide tuvastamine

Privaatsus: vabatahtlik, minimeeritud andmetöötlusega

3

Põhiõigused ja massandmetöötlus

- Seaduses sätestatud korras saab rahva tervise tagamiseks piirata inimeste vaba liikumist (PS § 34 l 2) või töödelda eraelulist teavet (PS § 26 l 2).
- Oluline on mõista, et mõned vabadused saab pärast riivet taastada, teisi aga mitte.
 - Liikumispiirangute täies mahus lõppemise järel on võimalik isikul jätkata liikumist ning tema vabadus on taastatud piirangutele eelnevaga võrdsele tasemele.
 - Eraelu puudutava teabe kolmandatele isikutele kättesaadavaks tegemist ei saa aga tagasi võtta: need isikud ei saa käsu peale teavet unustada. Näiteks võib tervishoiutöötajal olla raske unustada mõne tuntud isiku tervises seisundi teavet, mis talle teatavaks on saanud.

Asukohaandmete analüüs kriisis

- 24. märts 2020 teatab Statistikaamet, et hakkab liikumispiirangute jälgimiseks inimeste mobiiltelefonide asukohaandmeid töötleva.
- 30. märts 2020 täpsustatakse, et inimeste liikuvuse analüüs aitab teha otsuseid liikumispiirangute tugevdamise/nõrgendamise kohta.
- 1. aprill 2020 kirjutab Postimehe ja teaduste akadeemia liikmete nõukoda, et mobiiltelefonide asukohaandmetele ligipääsu andmisega viivitamine on mäng inimesteludega.
- 9. aprill 2020 teatas Statistikaamet tulemustest – inimesed püsivad rohkem kodus.

„Statistikaamet hakkab...” <https://www.err.ee/1068185/statistikaamet-hakkab-viiruse-leviku-piiramiseks-inimeste-liikumist-jalgima>

„Liikumisandmed aitavad otsustada...” <https://www.err.ee/1071067/amet-liikumisandmed-aitavad-otsustada-kuidas-ja-millal-piiranguid->

„...on mäng inimesteludega” <https://heureka.postimees.ee/6939107/postimehe-ja-akadeemikute-noukoda-andmetega-viivitamine-on-mang-inimesteludega>

„...püsivad inimesed rohkem kodus” <https://www.err.ee/1075441/statistikaameti-andmetel-pusivad-inimesed-rohkem-kodus>

Kuidas analüüs läbi viidi?

- Esialgse plaani järgi andmeid kogutaks kõikide mobiiltelefonide kohta.
- *„Ei viida läbi jälitustegevusega, tegemist ei ole isikustatud andmetega. Need on anonümiseeritud andmed. Eesmärk on anda pilt Eestis toimuvast liikumisest. Suuresti see töö toimub operaatorite majades, et tagada täielik anonüümsus. See ei ole reaalaaja andmestik, see on võrdlus enne eriolukorda ja pärast.“* --- Statistikaamet
- Teaduslikult on näidatud, et tavatööriistadega (*state-of-the-art*) on liikuvusandmete anonüümsust tagada peaaegu võimatu.
- Kirjeldatud lahendus viitab födereeritud statistikale, kuid ei ole selge, millised andmed üle anti ja kas need olid anonüümsed.

Lähikontaktide tuvastuse uuendused

- Märts 2020 – otsitakse innovatsiooni haiguse tõkestamises.
- Lõuna-Korea ehitab privaatsust tugevalt riivava platvormi karantiinis olijatele (mobiiliandmed, makseandmed, kaamerate andmed).
- Iisrael kavandab lähikontaktide tuvastamise nutitelefonide ja GPS-ga.
- Norra teeb sellise rakenduse ka päriselt ära (ka Bahrein, Kuveit).
- Singapuri TraceTogether rakendus on Bluetooth-põhise lähenemisega uudne, sest saab hakkama ilma GPS-ita.
 - Aga see ei tööta iPhone'idel, sest Apple'i telefonide privaatsuspiirangud segavad Bluetooth raadio kasutamist kasutajale nähtamatult.

Lõuna-Korea: Park S, Choi GJ, Ko H. Information Technology–Based Tracing Strategy in Response to COVID-19 in South Korea—Privacy Controversies. JAMA. 2020;323(21):2129–2130. <https://jamanetwork.com/journals/jama/fullarticle/2765252>

Iisrael: <https://www.forbes.com/sites/zakdoffman/2020/03/14/coronavirus-spy-apps-israel-joins-iran-and-china-tracking-citizens-smartphones-to-fight-covid-19>

Norra: <https://www.digi.no/artikler/smitteappen-ikke-trygg-nok-for-deler-av-forsvaret/490239>

Bahrein, Kuveit: <https://www.amnesty.org/en/latest/news/2020/06/bahrain-kuwait-norway-contact-tracing-apps-danger-for-privacy/>

Singapuri TraceTogether: <https://www.tracetogether.gov.sg>

Aprill 2020: privaatsust säilitama!

- Märtsi lõpus lubab Saksamaa-põhine PEPP-PT konsortsium lähikontakti tuvastuse rakendust, mis kasutab samuti Bluetooth-raadiosignaale.
- 4. aprill 2020 avaldab Šveitsi EPFL ülikooli [DP-3T](#) projekt konkreetse tehnilise hajusa lähikontakti tuvastuse lahenduse mobiiltelefonidele.
- 8. aprill 2020 DP-3T ja PEPP-PT lähevad tülili, algab „hajus vs keskne“ tüli.
 - Keskne küsimus – kas teenuseosutaja peaks saama teada inimeste kõik kontaktid?
 - Tsentraalseid rakendusi toetasid Inglismaa, Saksamaa, Prantsusmaa, Singapur.
 - Hajusaid rakendusi toetavad turbe-, õigus- ja privaatsusteadlased.
- 10. aprill 2020 tulevad Apple ja Google välja Exposure Notification APIga, mis aktiivselt takistab tsentraliseeritud rakenduste arendust.
 - Aluseks võetakse DP-3T projekti hajus lähenemine.

Privaatsus võitis, aga mis oli hind?

- Mais 2020 Apple/Google tarnivad Exposure Notification (GAEN) API toega telefonide operatsioonisüsteemid.
- Tsentraliseeritud lähikontaktide tuvastamist pooldanud riigid vaidlevad Apple'i ja Google'iga, et need ei takistaks riikidel juurutada rohkem andmeid koguvat lähenemist.
- Saksamaa, Inglismaa vahetavad tsentraliseeritud lähenemise GAENi hajusa vastu. GAEN abil ehitavad rakendusi ka paljud teised riigid.
- Võib väita, et sellel korral tegid suurfirmad õiget asja ning toetasid IKÜM printsiipe (andmetöötuse kahandamine, lõimprivaatsus), aga nende “võim” riikide üle on siiski murettekitav.

Andmekaitse “rahuajal”

Kuidas saada massandmeid?

- Õigusaktid sisaldavad mitmeid õiguslikke aluseid, sobiva puudumisel:
- **...võib proovida kirjutada uue seaduse või muuta vana,**
 - Sobib nii teenuste kui massandmetöötluste otstarbeks.
 - Kättesaadav (üldjuhul) vaid riigile.
- **... võib võtta isikult tema andmete töötlemiseks nõusoleku,**
 - Võimas vahend, toimib üle piiride ja ka delikaatsete andmetega.
 - Samas ei saa nõusolekuga kasutada terve populatsiooni andmeid.
- **... või püüda kasutada mõnda sobivat erandit.**
 - Näideteks on teadustöö, riiklik statistika – aga millised on anonüümimise nõuded?
 - Aga kui me tahame anda riigijuhtidele otsuste toeks andmeid (inimeste liikuvus)?
 - Aga kui me tahaks anda andmetele teisest kasutust nt tervishoiuvaldkonnas?

Segadus anonüümimise mõistega

- **Andmeteaduse mõistes** tähendab andmestiku anonüümimine selle teisendamist nii, et sealt isiku tuvastamine on keerukam.
 - Samas on tihti võimalik nii töödeldud andmestikust isikut tuvastada keerukamate andmeteaduse meetoditega või siis andmeid mõne teise kättesaadava andmestikuga sidudes.
- **Õigusliku mõistena** saab anonüümimist defineerida IKÜM põhjenduspunktist 26 tuletatud lihtsustatud selgituse järgi.
 - „Anonüümimine“ tähendab andmestiku muutmist nii, et sellest ei ole võimalik mõistlike pingutustega tuvastada ühtegi isikut.
- Andmeteaduse ja IKÜM arusaam sõnast “anonüümne” on erinev.

Näide anonüümimise piiridest

- Olgu osapoolel A biomeetriline andmekogu, millest on eemaldatud isikustavad tunnused ja pseudonüümid (andmestik on “anonüümne”).
- Eeldame, et alles on jäänud biomeetrilised tunnused (sõrmejälg, geenijärjestus, foto) ja näiteks ka mõni sisuline tunnus.
- Osapool A saab koguda avalikest allikatest (fotod, sõrmejäljed, kitkutud juuksekarv jne) biomeetria ning kontrollida, kas see on andmebaasis.
- Kui vastavus leitaks, siis on vastav kirje andmekogus isikustatud ning andmekogu pole anonüümne õiguslikus mõttes.
- Seega peame anonüümsuse tagamiseks piirama ligipääsu toorandmetele ning ka neil tehtavaid toiminguid.

Mis on “anonüümimisest tugevam”?

- Krüptograafia on matemaatiline distsipliin andmete teisendamiseks loetamatule kujule ja (sobiva võtme olemasolul) tagasi.
- **Tees 1:** kui ühel osapoolel on korrektselt krüpteeritud andmestik ja vastav võti, on andmed tema jaoks pseudonüümsed IKÜM põhjenduspunkt 26 mõistes.
- **Tees 2:** kui ühel osapoolel on korrektselt krüpteeritud andmestik, aga tal ei ole ligipääsu võtmele, siis on andmed tema jaoks anonüümsed IKÜM põhjenduspunkt 26 mõistes.
- Tänapäevase tehnoloogiatasemega on korrektselt teostatud krüptograafia murdmise töö palju suurusjärke mahukam kui andmeteaduse meetoditega anonüümitud andmete taasisikustamine.

IKÜM on innovatiivne – kasutagem!

- Kui ehitame “rahuajal” riigi valitsemist toetavad ja rahva tervist kaitsvad lahendused, toetavad need meid ka kriisi ajal ning ei nõua eraelu kaitse põhiõiguse riivet.
- IKÜM art 25 kehtestab vastutavatele töötlejatele lõimitud ja vaikimisi andmekaitse põhimõtete järgimise kohustuse.
 - See tähendab ka tehnoloogiatasemele vastavate privaatsuskaitse tehnoloogiate rakendamist.
- Selleks, et juurduks isikuandmete privaatse töötlemise kultuur, võiks avalikustada töötlemisel rakendatud tehnilised kaitsemeetmed vähemalt kokkuvõtlikul kujul
 - Siis ei peaks avalikkus ka mõistatama, mida tähendab, kui mõni süsteem väidab end töötlevat anonüümitud andmeid.