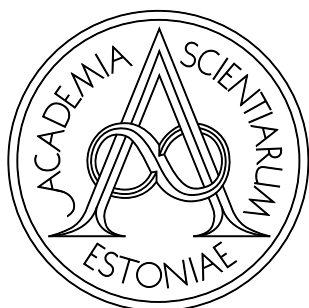




Teaduste akadeemia küberturvalisuse komisjoni koosoleku protokoll 21. jaanuaril 2026. aastal

Akadeemia majas Kohtu 6, Tallinn ja Zoomi keskkonnas

Algus kell 10.30

Lõpp kell 14.30

Juhatas akadeemik Dan Bogdanov

Osalesid: Irina Klementi, Ott Velsberg, Ahto Truu, Jan Villemson, Mauno Pihelgas, Eleri Karu, Andra Siibak, Kaisa Vooremäe, Riivo Talviste, Markko Liutkevičius, Tanel Tammet, Priit Vinkel, Irina Klementi, külalisena Kristjan Tops RIKist ja Allar Laaneleht Justiits- ja Digiministeeriumist

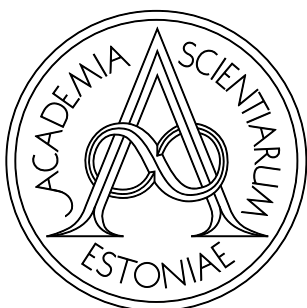
Puuduvad akadeemik Anu Realo, akadeemik Krista Fischer, Liiri Oja

Protokollis: Ülle Sirk

1. Mis tehtud, mis teoksil

Osalevad kõik kohalviibijad.

- a) Akadeemik Dan Bogdanov mainib, et me oleme sisenenud riigi korraldatud konverentside aega. Eile toimus tehisaru konverents, kohe on tulemas küberkaitsekonverents, seejärel on tulemas Võrdõigusvoliniku konverents, siis inimõiguste konverents. Kõikide nende sisuline pool puudutab meie komisjoni tööd. Kuidas hinnata toimunud tehisaru konverentsi, mille korraldas Justiits- ja Digiministeerium, komisjoni liikmed mitmed osalesid?
- b) Priit Vinkel möönab, et üritus oli mitmepalgeline, sai erinevat infot, selgusetuks ehk jäi, mis oli oodatud sihtrühm ja mis oli kasutegur. Tundub, et ootus oli defineerimata, mistõttu jäi see kuulajale häguseks.
- c) Mauno Pihelgas ja Eleri Karu on sellega nõus, et vastamata jäi küsimus, mida teha edasi. Eleri Karu kiidab lõpupaneeli, kus noored rääkisid tehisaru kasutamisest, kus oli väga aus lähenemine. Markko Liutkevičius kiidab samuti konverentsi sisulist teostust.
- d) Järgmisele teemale minnes, Eleri Karu markeerib, et muret on tekitamas riigi veebilehtedel asuvad teenused, kus saab isikukoodi teades teha autentimata päringuid. Muret on tekitamas ka infosüsteemide ehitus, kus on kaasatud mõnede kolmandate riikide tarkvaraarendajad.
- e) Irina Klementi sekundeerib, et viimane teema on laual ka Justdigi ministeeriumis ja soovitakse tellida õiguslikku hanget selle probleemi lahendamiseks.



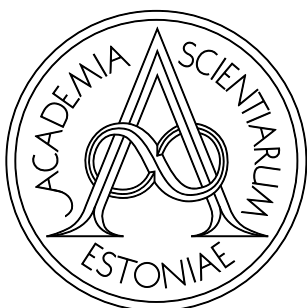
- f) Akadeemik Dan Bogdanov ütleb, et see küsimus tuleb ka küberturvalisuse komisjoni tarneahela riskianalüüsis arutelu alla, veel täna.
- g) Jan Willemson selgitab põhjalikult oma 20.01 ERRis ilmunud tehisintellekti toetatud hariduse üle arutleva artikli sisu tagamaid.
- h) Akadeemik Dan Bogdanov ja tehisaru jaaju komisjonist Liina Kamm esinesid koolis samadel teemadel õpetajaskonnale ja õhku jäi küsimus, kas valeinfot esitava juturoboti kasutuselevõtul saab kahjustada õpetaja autoriteet, kui ta ütleb, et tõde on teistsugune?

Informatsioon võeti teadmiseks.

2. Riskianalüüsides. Oleme alustanud ohtude kirjapanemist ja mõned hakkavad jõudma kontrolli faasi.

Osalevad kõik kohalviibijad.

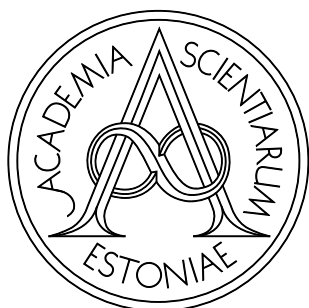
- 1) AIJURIST kvaliteedikontroll: Vähekindlustatud isikute õigusabiteenuse tehisintellektile üle viimine rikub teenuse kvaliteeti ja põhjustab kahju seda kasutavale isikule
 - a) Markko on teinud tekstis muudatusi, mida ta tutvustab—ta parandas faktilisi andmeid. Tal oli kättesaadav õiguslik mõjuhindang, täiustas seda selles kontekstis, tegemist ei ole õigusnõu andmisega, vaid õigusinfo esitamisega. Oluline on, kuidas tagatakse AI täpsus ja usaldusväärsus. See on tähtis, et teada, kuidas kvaliteeti kontrollitakse järjepidevalt ja kuidas on tagatud privaatsus. Taustal on inimesed, kes teenust kontrollivad, kes võivad kokku puutuda isikuandmetega, nad on lepingupartnerid ja see on kontrollitud tegevus. Olulised on kasutajasõbralikkus ja ligipääsetavus. Loodud on kasutamise juhendid, mida on plaanis saata raamatukogudele. Juturobot pakub teenust teisel moel kui seda teeks nõustaja.
 - b) Allar Laaneleht selgitab teemat põhjalikumalt. Tegu ei ole õigusnõustajaga vaid õigusteabe juturobotiga. On määratud, mis on riigi toetav õigusnõustamine ja roboti tegevus sellele ei vasta. Juturobot kasutab andmetena Riigi Teataja materjale, lähiajal lisatakse Riigikohtu lahendeid ja ka kohalike omavalitsuste materjale. Kvaliteedikontrolli jaoks on sõlmitud leping Eesti Juristide Liiduga, kes kontrollib neid vestlusi. Inimesed saavad juturobotit kasutada ka raamatukogudes. Inimeste toetamiseks on raamatukogudele tehtud juba tutvustus, kuidas robotit kasutada, kuid neile ei teki kohustust aidata kasutajatel küsimusi formuleerida ega roboti vastuseid hinnata. Oleme välise ja sõltumatu partneriga loomas protseduuri, millega saame ajas mõõta ja hinnata juturoboti kvaliteeti.
 - c) Jan Villemson tõstatab vastutuse küsimuse—kes vastutab, kui inimene saab juturobotilt vale info ja teeb selle põhjal midagi?



- d) Allar Laaneleht ütleb, et juturobot algul kui lõpus annab teada, et ta on robot ning kutsub ka üles vastuseid ise üle kontrollima. Juturobot toetab oma väljundit viidetega allikatele. Senine tasuta õigusnõustamine jääb alles haavatavatele gruppidele, nt puuetega inimestele ja eakatele.
- e) Eleri Karu AKIst toonitab, et üles peab minema info isikuandmete mitte kasutamisest, see on tungiv soovitus. Allar kinnitab, et dokumente (faile) lisada ei saa ning juturoboti tervitussõnum keelab isikuandmete sisestamise vestlusaknasse. Teenuse toimimise jaoks ei ole isikuandmete sisestamine ning nende töötlemine vajalik. Samuti on juturoboti kasutusjuhises pühendatud peatükk andmekaitsele ja privaatsusele. Inimestelt ei oodata sisendis isikuandmete lisamist, kuid kui neid sisestatakse, siis on robot seadistatud käituma viisil, mis oma vastuses isikuandmeid tagasi ei “peegelda”. Sellest hoolimata kustutatakse küsimused teatud aja tagant. Indrek Tops RIKist räägib, et hetkel on ülevaatomisel ka privaatsustingimused, mille kohaselt kustutatakse 3 kuu jooksul isikuandmeid sisaldavate vestluste sisu.
- f) Akadeemik Dan Bogdanov nendib, et seni analüüsis komisjoni ohtu õigusabi teenuse kontekstis, aga nüüd vaatame tehtu üle õigusinfo teenuse kontekstis. See on oluline muudatus käsitusallas. Kahju, et süsteemi esmane kirjeldus jättis mulje, et tegemist on õigusabi teenusega.
- g) Jan Villmeson toonitab, et inimesele tuleb anda kontrolli meetodika. Anda talle abilingid ja muu täiendav info. Suurim kahju on usalduse küsimus—kui inimene esimesel korral saab valeabi, ta ei usalda süsteemi enam.
- h) Eleri Karu ootus on, et teenus kasutaks tulevikus ka otsekohalduvaid Euroopa Liidu määruseid.

Otsustati, kuna kvaliteedikontrolliks tekkis juurde palju uut materjali, tuleb teemaga edasi tegeleda.

- 2) **ÕPILANGUS** kvaliteedikontroll: Suurte keelemudelite laialdane rakendamine üldhariduses viib õpioskuse ja iseseisva mõtlemise languseni
 - a) Eleri märgin ära, et äsja on ilmunud OECD aruanne tehisintellekti rollist õppetöös ning see võiks olla kasulik allikas.
 - b) Jan Villemson leiab, et meie praeguse ohukirjelduse kaitsemeetmed on deklaratiivsed ja kas on võimalik üldse midagi lisada? Ott Velsberg leiab samuti, et kaitsemeetmed on praegu nõrgalt sõnastatud. Akadeemik Bogdanov innustab komisjoni tööd parandama.
 - c) Ott Velsberg toob esile teenuse muutumise ohu nii, et kasutaja ei saa teada sellest muudatusest. Kui alusmudel muudetakse, on sel võimalik negatiivne mõju teenuse kvaliteedile ja ohutusele. Akadeemik Dan Bogdanov nõustub, et see vajab käsitlemist, kuid kvaliteedi ja õpilanguse vaatepunktist. Mudeli tervikluse küsimuse jaoks peame sõnastama eraldi



ohusündmuse. Oluline on, et oleks vajadusel olemas alternatiivne teenusepakkuja.

- d) Andra Siibak küsib, kas oleks õpetajatele vaja täiendavat didaktilist tuge? Kuidas saab õpetaja lisada loomingulist lähenemist? Jan Villemson on kriitiline õpiringide kasuteguri suhtes, puudub ühine metoodika ja abi on loota vaid teistelt õpetajatelt, kes on midagi avastanud.
- e) Tanel Tammet nendib, et puudub piisav riigi kui ka eraraha tugi ning see hoiab algatust tagasi.
- f) Jan Villemson leiab, et rahastuse valguses on oluline arenduse läbipaistvus. TI-hüpet arendatakse osaliselt ka avaliku raha peal ja üks eeldusi on, et tekiks avalik kontroll. See hakkab mõjutama väga suurt osa ühiskonnast. Ott Velsberg toonitab, et eraraha ei ole olnud lihtne kaasata.
- g) Jan Villemson nendib, et tehisintellekt ei tea koolides kasutatavat terminoloogiat ega tähistusi, et tea Eesti kirjandust jne. Akadeemik Dan Bogdanov nõustub, et kasutatava sõnavara seisukohalt on olulised õpikud—peame saama TI-hüppele külge õppekavad ja õpikud. Tekib keerukas õpikute intellektuaalomandi küsimus, kirjastuste vara kaitse tuleb tagada. Järgnenud arutelust jääb kõlama, et mitmed õpikud on rahastatud riigi poolt, õppekavad kehtestatakse riiklikult. Aga kiiret lahendust ei ole. Ahto Truu toob välja, et kogu Eesti kirjanduse viitamist ei saa tehisintellektilt praktikas oodata kasvõi on takistuseks erinevate aastate trükid kohustuslikust kirjandusest.
- h) Sedastatakse, et AIJURIST ohukirjelduses viidatud õigusteab teenus on täna erialase algmaterjali ja tõese infoga paremini liidestatud kui TI-Hüppe teenus.

Informatsioon võeti teadmiseks ja ohukirjelduse täiendamise jätkub.

- 3) PAHAKOOD mustandi ülevaatus: Riigi e-teenuses kasutatava tarkvarakomponendi haavatavuse või tagaukse tõttu on häiritud elutähtsa teenuse terviklus
 - a) Komisjoni esimees selgitas, et selle ohukirjelduse alge kirjutas Irina ja nüüd on üldise tarneahela riski alamosa (tarkvara terviklus) lahti kirjutanud Kaisa, Irina ja Ahto. Fookuses on elutähtsate teenuste ja andmete terviklus. Tekkida võivad ka konfidentsiaalsuse kadu ja tervikluse kadu, kui andmetesse satuvad manipuleeritud andmed. See võib tekitada ohu riiklikule julgeolekule ja usalduse kao e-riigi vastu. Meie keskendume riiklikele e-teenustele. Pole vahet, kas ründaja on tarkvaraarendaja, oht tuleb seestpoolt või väljaspoolt (tarkvarauuendus, mida ei jõuta läbi kontrollida). Järgnes arutelu.
 - b) Aastaid on räägitud, kas peaks hangetes olema turvanõuded arendusele ja protsessidele, aga see tõstaks ilmselt arendustunni hinda. Turvateadlik hankepoliitika, sh kvaliteedi-ja teenustasemenõuded hankelepingutes, on Eestis arengujärgus.

- c) Probleem ei ole mitte ainult tarkvarauuendustes vaid ka esmases tärnes, mida ei jõuta kontrollida rohkem kui läbistustestidega, mis ei kata samas tarkvara terviklust.
- d) Ainus valdkond, kus Eestis ostetakse sertifitseeritud lahendusi, on digitaalne identiteet, mujal turvasihte ja standardeid pigem ei käsitleta.
- e) Tavapraktika on, et probleemid jõuavad infoturbejuhuini ja edasine sõltub tema kompetentsist. RIA seireandmed on täpsustamisel, järgmisel koosolekul saab neid põhjalikumalt arutada

Otsustati jätkata ohukirjelduse täiustamisega.

- 4) Hindamisskaala arutelu: Oht riigikorrale või sotsiaalmajanduslikule olukorrale
 - a) Komisjon vaatas üle seni tehtud töö hindamisskaala arendamisel ning nentis, et kõige raskem on mõõta kahjude ulatust (kui palju inimesi mõjutatud on, näiteks).
 - b) Jan Villemson mainib, et mõõdikutel võib olla palju põhjuseid. Kas peaksime hakkame filtreerima, et milline osa on just selle sündmuse tagajärg. Näiteks SKP, hinded ja EMO külastatavus on hästi mõõdetavad, aga milline on baastase?
 - c) Jan tõi välja ka, et tihti kasutatav lineaarne protsendijaotus (0% -- 20%, 20%-40% populatsioonist jne) ei toimi vaja oleks eksponentsiaalsemat skaalat.
 - d) Irina Klementi pakkus majandusliku mõõdikuna välja SKP muutuse või kõikumise, protsentides.
 - e) Komisjoni esimees leiab, et oluline on ehitada sündmuse ahel, nt õpilased käivad AI alt läbi, sisenevad selle järel tööturule ja nende tulemused on tuntavalt madalamad. Kas suudame öelda, et mingi üks protsess on määravam?
 - f) Komisjoni esimees akad Bogdanov tegi ettepaneku leida kontakt Riigikantsleiga, kus koostatakse riiklikku riskianalüüsi.

Otsustati konsulteerida Riigikantsleiga, kelle riskianalüüsis on mitmed sarnased teemad käsitletud.

Järgmise koosoleku aeg

Järgmine koosolek toimub 26. veebruaril 2026 Tartus, Narva mnt 20, Cybernetica ruumides

