Näotuvastusega saab võimaldada kuhugi sissepääsu, kuid enam levinud on see telefoni sisselogimiseks.

Andmekaitse ekspert Tõnu Metsäär: ärge koguge töötajate biomeetrilisi andmeid

Intervjueeris: **Jaanika Palm**

Amsterdamist on pärit kaasus, kus tööandja paigaldas töötajatele kassaaparaadi avamiseks sõrmejäljelugeja, selleks et vältida vargusi. Menetluse käigus langes süü tööandjale, sest ta ei olnud kaalunud töötajate privaatsust vähem rikkuvaid alternatiive biomeetriliste isikuandmete kogumisele.

Waldrand Law OÜ juhataja ja andmekaitse ekspert (GDPR24.ee) Tõnu Metsäär selgitab, mida peab tööandja teadma biomeetriliste isikuandmete kogumisest ja töötlemisest.

Mis on biomeetrilised andmed?

Eestis kohustusliku Euroopa Liidu isikuandmete kaitse üldmääruse ehk GDPRi järgi on biomeetrilised isikuandmed tehniliste vahendite abil saadavad andmed inimese füüsiliste, füsioloogiliste ja käitumuslike omaduste kohta, mis võimaldavad seda inimest kordumatult tuvastada.

Kui meie siin kaitseme kiivalt isikuandmeid, siis Hiinas saab näotuvastuse alusel osta ka praekana.

Biomeetrilised isikuandmed on n-ö eriliigilised – privaatsust kõige enam riivavad. See tähendab ühtlasi, et nad vajavad võrreldes tavaliste isikuandmetega tugevamat kaitset. Levinumad biomeetriliste andmete kasutamisviisid on isiku tuvastamine näokujutise või sõrmejälje abil ning silmaiirise skannimine.

Biomeetrilised isikuandmed on igale isikule ainuomased ja kordumatud. Nagu näiteks ka unikaalsed kehalõhnad, kõrva kuju või mõni käitumuslik omadus – kuidas keegi kõnnib või istub.

Milleks biomeetrilisi andmeid kasutada saab?

Isikutuvastust näo- ja sõrmejälje põhjal kasutatakse praegu peamiselt mitmetesse seadmetesse, näiteks nutitelefonisse sisselogimiseks. Ka selleks, et võimaldada kuhugi sissepääsu.

Kas tööandjate soovid biomeetriliste andmete kogumiseks ja kasutamiseks on põhjendatud ja eesmärgipärased?

Igasuguste isikuandmete, sh biomeetriliste isikuandmete kogumise ja töötlemise puhul on eesmärgipärasus ja andmete minimaalse kogumise põhimõtted kõige olulisemad.

Biomeetriliste isikuandmete töötlemine on GDPRi artikli 9 järgi keelatud. Olemas on ka erandid, mis sealsamas artiklis on välja toodud. Üks neist eranditest on inimese selgesõnaline nõusolek tema isikuandmete töötlemiseks.

Nõusolekut tähtsustakse sageli aga üle. Nõusoleku võib alati tagasi võtta ning siis jääb andmete töötlemine õigusliku aluseta, muutub ebaseaduslikuks.

Mida peab tööandja teadma, kui ta soovib koguda töötajate biomeetrilisi andmeid?

Tööandjate jaoks on olukord Eestis väga keeruline, sest Euroopa Andmekaitsenõukogu on oma juhistes välja toonud, et töösuhetes isikuandmeid nõusoleku alusel töödelda ei või. GDPRi järgi peab nõusolek isikuandmete töötlemiseks olema antud vabatahtlikult, kuid töösuhtes ei ole tööandja ja töötaja võrdses positsioonis. Töötaja vaba tahe on töösuhte puhul küsitav. Töösuhete puhul arvestatakse töötajaga kui nõrgemas positsioonis olijaga.

Seega – töösuhtes langeb töötaja nõusolek isikuandmete töötlemiseks ära. Samuti puudub meil vastav õigusaktist tulenev eraldi õiguslik alus, mis näiteks Hollandis ja Prantsusmaal on nende andmete töösuhtes töötlemise jaoks olemas.

Toon siia näite Islandi kahe aasta tagusest kaasusest, kus tööaja arvestussüsteemis kasutati töötaja tuvastamiseks tema sõrmejälge ning kohalik andmekaitse järelevalveasutus leidis GDPRi põhjenduspunktidele 42 ja 43 viidates, et tööandjal olid olemas küll töötajate nõusolekud, kuid töösuhtes nõusolekust biomeetriliste andmete töötlemiseks ei piisa.

Teine analoogiline näide on Hollandist, kus tööandjale tehti 725 000 eurot andmekaitsetrahvi töötajate sõrmejälgede ebaseadusliku kasutamise eest. See trahv on hetkel kohtus vaidlustatud.

Missugused tavad on teistes riikides?

Biomeetriliste andmetega on nii nagu paljude teiste uute tehnoloogiliste lahendustega. Kui „asjad" on kasutusele võetud ning inimesed on need omaks võtnud, siis sellele järgneb õiguslik reguleerimine. Erialast kirjandust lugenuna ei ole ma veendunud, et biomeetria jääb andmekaitse mõttes üldse käibesse. Isikute privaatsuse riive on liiga suur.

Hiinas on olukord aga teine. Kui meie siin kaitseme kiivalt isikuandmeid, siis Hiinas saab näotuvastuse alusel osta ka praekana.

Kuidas ja kui suures ulatuses siiski biomeetrilisi andmeid Euroopas kasutada võib, selgub lõplikult ehk siis, kui on olemas piisavalt kohtulahendeid. Praegu see nii veel ei ole.

Kas tööandjal on õigus töösuhte kestel töötaja biomeetrilisi andmeid ühtäkki nõudma hakata? Näiteks olukorras, kus ettevõte täidab tellimust, millega seotud andmeid loetakse riigisaladuseks ja ta peab kindlasti teadma, et kõik oleks turvaline – kas see on piisav põhjus hakata oma töötajaid tuvastama biomeetriliste isikuandmete põhjal?

Selline nüanss on tõepoolest olemas. GDPRi artikli 2 punkt 2(a) ja seda täpsustav põhjenduspunkt 16 ütlevad, et üldmäärust ei kohaldata, kui isikuandmeid töödeldakse riigi julgeoleku tagamisega seotud tegevuste käigus.

Siiski rõhutan veel, et hoolimata kõnealusest erisusest peab olema põhjendatud vajadus koguda ja töödelda isikuandmeid just sellisel moel. Alati tuleb lähtuda eesmärgipärasuse ja vajaduse põhimõttest. Tuleb kaaluda, kas on võimalik kasutada töötaja privaatsust vähem riivavaid turvameetmeid ning kui ei ole, siis miks ei ole. Need vastused peavad tööandjal läbi mõeldud ja tõendatavalt olemas olema, muu hulgas ka kohtu jaoks, kui seda peaks vaja minema.

Oluline on rõhutada kahte sätet Eesti põhiseadusest ja töölepingu seadusest. Eesti põhiseaduse paragrahv 26 sätestab, et igaühel on õigus perekonna ja eraelu puutumatusele. Töölepingu seaduse paragrahvi 28 punkt 11 ütleb, et tööandja peab austama töötaja privaatsust ja kontrollima töökohustuste täitmist viisil, mis ei riku töötaja põhiõigusi. Neist mõlemast kohustuslikust sättest tuleb tööandjal juhinduda ka biomeetriliste isikuandmete kontekstis.

Mida veel peaksid tööandjad töötajate isikuandmete töötlemisest teadma?

Biomeetriliste isikuandmete kogumine töösuhetes ei ole täna Eestis õiguslikult võimalik.

Teiseks tuleb alati läbi mõelda, miks isikuandmeid üldse kogutakse ja kuidas on need turvatud. See kõik tuleb tööandjal kui andmetöötlejal ka oma sisedokumentidesse kirja panna ja privaatsusteates (ingl privacy notice) oma töötajatele, klientidele ja partneritele avaldada.

GDPRi puhul on oluline rõhutada ka nn pööratud tõendamiskohustust. See tähendab, et kui näiteks süüteomenetluses peab riik tõendama teo toimepanemise asjaolusid, siis peab andmetöötleja olema valmis igal hetkel tõendama, et tema tegevus vastab andmekaitsenormidele. See on küllaltki erandlik olukord.

Mida andmekaitse eksperdina soovitate tööandjatel teha?

Minu soovitus on revolutsiooniliselt lihtne: ärge koguge töötajate biomeetrilisi andmeid. Nii saab vältida kõiki sekeldusi. ■