

Asia C-77/21

Ennakkoratkaisupyyntö

Jättämispäivä:

8.2.2021

Ennakkoratkaisupyyntön esittänyt tuomioistuin:

Fővárosi Törvényszék (Unkari)

Ennakkoratkaisupyyntön esittämistä koskevan päätöksen tekemispäivä:

21.1.2021

Valittaja:

Digi Távközlési és Szolgáltató Kft.

Vastapuoli:

Nemzeti Adatvédelmi és Információszabadság Hatóság (valtion tietosuojaviranomainen)

Fővárosi Törvényszék (Budapestin alioikeus, Unkari)

[– –]

Valittaja:

Digi Távközlési és Szolgáltató Kft. ([– –]
Budapest [– –])

[– –]

Vastapuoli:

Nemzeti Adatvédelmi és
Információszabadság Hatóság (valtion
tietosuojaviranomainen) ([– –] Budapest [–
–])

[– –]

Asian kohde:

Tietosuoja-asiassa tehdyn hallintopäätöksen
[– –] lainmukaisuuden arviointi

V ä l i p ä ä t ö s

Euroopan unionin tuomioistuimelta pyydetään ennakkoratkaisua seuraaviin kysymyksiin:

”1) Onko luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta 27.4.2016 annetun Euroopan parlamentin ja neuvoston asetuksen (EU) 2016/679 (jäljempänä tietosuoja-asetus) 5 artiklan 1 kohdan b alakohdassa tarkoitettua käyttötarkoitussidonnaisuutta tulkittava siten, että sen mukaisesti voidaan katsoa se, että rekisterinpitäjä tallentaa myös toiseen tietokantaan henkilötietoja, jotka on [alun perin] kerätty tiettyä laillista tarkoitusta varten ja tallennettu sen mukaisesti, vai onko päinvastoin katsottava, että tällaisen rinnakkaistietokannan osalta tietojen säilyttäminen ei ole enää tällaisen laillisen tarkoituksen mukaista?

2) Jos ensimmäiseen kysymykseen vastataan, että tietojen rinnakkainen tallentaminen on sellaisenaan vastoin tietosuoja-asetuksessa tarkoitettua käyttötarkoitussidonnaisuuden periaatetta, voidaanko tallentaminen katsoa tietosuoja-asetuksen 5 artiklan 1 kohdan e alakohdassa säädetyn säilytyksen rajoittamista koskevan periaatteen mukaiseksi, kun rekisterinpitäjä tallentaa [alun perin] määrättyä laillista tarkoitusta varten kerätyt ja tallennetut tiedot toiseen rinnakkaiseen tietokantaan?

[kansallisia prosessioikeudellisia seikkoja]

Perustelut

Tosiseikat

- 1 Valittaja on yksi Unkarin internet- ja televisiopalvelujen markkinoiden johtavista toimijoista.
- 2 Valittaja perusti testaamista ja virheiden korjaamista varten huhtikuussa 2018 testi-nimisen tietokannan (jäljempänä testitietokanta), johon se kopioi noin kolmanneksen yksityisasiakkaidensa henkilötiedoista. Toisessa, digihu-nimisessä tietokannassa, joka oli linkitetty digi.hu -sivustolle, se säilytti suoramarkkinointia varten päivitettyinä tiedotteensa tilaajien ja niiden järjestelmien järjestelmävastaavien tiedot, joilta oli pääsy internetsivustolle. **[alkup. s. 2]** Tässä tietokannassa oli henkilötietoja noin kolmesta prosentista sen yksityisasiakkaita ja neljänkymmenen sellaisen järjestelmävastaavan käyttäjätiedot, joilla oli joko täysi tai osittainen järjestelmän käyttöoikeus.
- 3 Valittaja sai 23.9.2019 tietää, että www.digi.hu-sivustolta oli päästy henkilötietoihin (nimi, äidin nimi, syntymäpaikka- ja aika, henkilötodistuksen numero tai joissain tapauksissa henkilötunnus, sähköpostiosoite ja kiinteän puhelimen ja matkapuhelimen numerot) noin 322 000 henkilön osalta (297 000 asiakasta ja tilaajaa sekä 25 000 tiedotteen tilaajaa). Tietokantaan murtautunut hakkeri ilmoitti itse kirjallisesti valittajalle hyökkäyksestä 21.9.2019 lähettämässään sähköpostiviestissä, johon se oli näytöksi koonnut yhden tietokannan rekistereistä ja jossa se teki selkoa vian teknisistä ominaisuuksista. Tämän jälkeen valittaja korjasi vian, teki eettisen hakkerin kanssa

salassapitosopimuksen ja tarjosi hakkerille palkkiota. Tietomurto ei kohdistunut digihu-tietokantaan, mutta tämä olisi ollut mahdollista.

4 Valittaja ilmoitti henkilötietojen tietoturvaloukkauksesta vastapuolelle 25.9.2019, ja tämä aloitti ilmoituksen johdosta virallisen tarkastusmenettelyn 8.10.2019.

5 Vastapuoli totesi 18.5.2020 tekemässään päätöksessä seuraavaa:

a) Valittaja on rikkonut tietosuoja-asetuksen 5 artiklan 1 kohdan b ja e alakohtaa, koska se ei ole testien ja virheiden edellyttämien korjausten jälkeen poistanut tietoturvaloukkauksen kohteeksi joutunutta testitietokantaa, joka oli perustettu alun perin virheiden korjaamista varten, eli se oli säilyttänyt testitietokannassa suuren joukon asiakkaiden henkilötietoja lähes puolentoista vuoden ajan ilman minkäänlaista tarkoitusta ja mahdollistanut sen, että henkilöt voitiin tunnistaa, ja mahdollisuus tietoturvaloukkauksen tapahtumiseen johtui välittömästi toimenpiteen (testitietokannan poistaminen) laiminlyönnistä.

b) Valittaja on lisäksi rikkonut tietosuoja-asetuksen 32 artiklan 1 ja 2 kohtaa.

Se velvoitti kantajan tarkistamaan kaikki henkilötietoja sisältävät tietokantansa siltä kannalta, oliko perusteita salaustoimenpiteiden suorittamiseen, ilmoittamaan vastapuolelle tämän selvityksen tuloksesta ja maksamaan 100 000 000 HUF:n suuruisen tietoturvasakon. Se määräsi päätöksensä julkaistavaksi.

6 Päätöksensä perusteluissa vastapuoli viittasi tietosuoja-asetuksen 2 artiklan 1 kohtaan, 4 artiklan 12 kohtaan, 5 artiklan 1 kohdan b ja e alakohtaan, 17 artiklan 1 kohdan a alakohtaan, 32 artiklan 1 kohdan a alakohtaan ja 2 kohtaan, 33 artiklan 1 ja 2 kohtaan sekä 4–5 kohtaan.

7 Se korosti sitä, että tietosuoja-asetus oli tullut sovellettavaksi Unkarissa 25.5.2018 alkaen ja että henkilötietojen tietoturvaloukkauksen kohteena ollut henkilötietojen käsittely (asiakkaiden henkilötietojen säilyttäminen) oli jatkunut tämän päivän jälkeen, minkä vuoksi tietosuoja-asetusta oli sovellettava asiassa sen 2 artiklan 1 kohdan ja 99 artiklan 2 kohdan nojalla.

8 Vastapuoli totesi, että testitietokannan perustamisen tarkoitus – testaaminen, virheiden korjaaminen – ei vastannut tarkoitusta, jota varten tietokantaan tallennettuja henkilötietoja alun perin käsiteltiin (sopimusveloitteiden täyttämisen), sillä virheiden tultua korjatuiksi oli poistunut myös tietojen käsittelyn varsinainen tarkoitus (testaus ja virheiden korjaaminen). Koska tietokantoja ei ollut virheiden korjaamisen jälkeen poistettu, asiassa oli näin syyllistytty tietojen säilytyksen rajoittamista koskevan periaatteen loukkaamiseen.

9 Tietojen säilyttämiseen kohdistettavien tietoturvatoimenpiteiden osalta se totesi ensisijaisesti, että tietoturvaloukkauksen voitiin katsoa johtuneen valittajan sisällönhallinnassa käyttämän Drupal -järjestelmän haavoittuvuudesta, josta oltiin jo pitkään oltu tietoisia ja joka olisi ollut korjattavissa, mutta valittaja ei tästä

huolimatta ollut korjannut kyseisen tietojärjestelmän puutteita, koska käytettävissä oleva korjauspaketti ei ollut virallinen. Asian käsittelyyn toimitettuun tietoturvaan koskevaan asiantuntijalausuntoon nojautuen vastapuoli korosti sitä, että tietoturvapuutteet olisi voitu korjata tähän soveltuvalla tietokoneohjelmalla ja haavoittuvuuteen säännöllisesti kohdistettavilla valvontatoimenpiteillä ja asianmukaisilla salaustoimenpiteillä, ja totesi, että laiminlyömällä nämä toimenpiteet valittaja oli toiminut tietosuoja-asetuksen 32 artiklan 1–2 kohdan vastaisesti.

- 10 Vastapuoli velvoitti valittajan maksamaan tietoturvasakon tietosuoja-asetuksen 83 artiklan 2 kohdan ja henkilötietoihin liittyvästä määräämisoikeudesta ja tiedonvälityksen vapaudesta vuonna 2011 annetun lain nro CXII (az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII törvény, jäljempänä tietosuojalaki) tiettyjen säännösten nojalla.

Pääasia

- 11 Valittaja on riitauttanut vastapuolen päätöksen valituksellaan [ennakkoratkaisua pyytävään tuomioistuimeen]. [alkup. s. 3]
- 12 Valittaja on tuonut käyttötarkoitussidonnaisuuden periaatteen osalta esiin sen, että tietoturvaloukkauksen kohteena oleviin tietokantoihin siirretyt asiakkaiden henkilötiedot oli kerätty lainmukaisesti tilaussopimusten tekemistä varten tietosuoja-asetuksen 6 artiklan 1 kohdan b alakohdan mukaisesti, eikä tämä käyttötarkoitus muuttunut tietoturvaloukkauksen kohteeksi joutuneita testitietokantoja perustettaessa. Valittaja oli perustanut testitietokannat säilyttääkseen tiedot, jotta sillä olisi ollut ne käytössään sitä alkuperäistä lainmukaista tarkoitusta varten, johon ne kerättiin. Tämän vuoksi testitietokantojen perustaminen eli se, että kerättyjä tietoja säilytetään jossakin toisessa sisäisessä tietojärjestelmässä, ei ole ristiriidassa tietojen keräämistarkoituksen kanssa. Valittajan mukaan käyttötarkoitussidonnaisuuden periaate ei kerro sitä, mikä on se sisäinen tietojärjestelmä, jossa järjestelmävastaavalla on lupa käsitellä lainmukaisesti kerättyjä tietoja, niin kuin se ei myöskään kiellä kopioimasta lainmukaisesti kerättyjä tietoja. Valittaja väittää, että käsiteltyjen henkilötietojen ala ei laajentunut testitietokantojen perustamisella ja että vaikka testitietokannan perustaminen tai säilyttäminen on mahdollisesti lisännyt tietoturvariskejä, tätä ei kuitenkaan voida katsoa kyseisen perusperiaatteen loukkaukseksi, vaan korkeintaan kysymys on tietosuoja-asetuksen 32 artiklassa tarkoitettusta tietoturvaan liittyvästä tilanteesta. Se katsoo, että säilyttämällä myös testitietokannassa tällaiset lailliseen tarkoitukseen kerätyt tiedot ei rikottu tietosuoja-asetuksen 5 artiklan 1 kohdan b alakohtaa.
- 13 Säilytyksen rajoittamista koskevan periaatteen osalta valittaja on esittänyt, että asiakastietojen käsittelyn tarkoituksena ei ollut virheiden korjaaminen, minkä vuoksi tietojen säilytysaikaa ei voitu sovittaa virheiden korjaamiseen tarvittuun aikaan. Säilytyksen rajoittamisvaatimusta ei näin ole sivuutettu sillä, että

testitietokantaa ei poistettu heti virheiden korjaamisen jälkeen, koska valittajalla oli oikeus säilyttää tietoja testitietokannassa, jossa se voisi yksilöidä asianomaiset henkilöt virheiden korjaamisesta riippumatta. Valittajan ei näin ollen voida katsoa millään tavoin syyllistyneen tietosuoja-asetuksen 5 artiklan 1 kohdan e alakohdan rikkomiseen.

- 14 Valittaja on vaatinut ennakkoratkaisupyynnön esittämistä unionin tuomioistuimelle muun muassa edellä kuvatun kysymyksen osalta.
- 15 Vastapuoli on vaatinut valittajan valituksen hylkäämistä. Se katsoo, ettei asiassa ole kysymyksiä, joiden vuoksi ennakkoratkaisua olisi pyydettävä.

Asian kannalta merkityksellinen unionin oikeus

- 16 Tietosuoja-asetuksen 5 artiklan 1 kohdan b alakohdassa, joka koskee henkilötietojen käsittelyn periaatteita, säädetään, tiedot on kerättävä tiettyä, nimenomaista ja laillista tarkoitusta varten, eikä niitä saa käsitellä myöhemmin näiden tarkoitusten kanssa yhteensopimattomalla tavalla; myöhempää käsittelyä yleisen edun mukaisia arkistointitarkoituksia taikka tieteellisiä tai historiallisia tutkimustarkoituksia tai tilastollisia tarkoituksia varten ei katsota 89 artiklan 1 kohdan mukaisesti yhteensopimattomaksi alkuperäisten tarkoitusten kanssa ("käyttötarkoitussidonnaisuus").
- 17 Tietosuoja-asetuksen 5 artiklan 1 kohdan e alakohdan mukaan on säilytettävä muodossa, josta rekisteröity on tunnistettavissa ainoastaan niin kauan kuin on tarpeen tietojenkäsittelyn tarkoitusten toteuttamista varten; henkilötietoja voidaan säilyttää pidempiä aikoja, jos henkilötietoja käsitellään ainoastaan yleisen edun mukaisia arkistointitarkoituksia taikka tieteellisiä tai historiallisia tutkimustarkoituksia tai tilastollisia tarkoituksia varten 89 artiklan 1 kohdan mukaisesti edellyttäen, että tässä asetuksessa vaaditut asianmukaiset tekniset ja organisatoriset toimenpiteet on pantu täytäntöön rekisteröidyn oikeuksien ja vapauksien turvaamiseksi ("säilytyksen rajoittaminen").

Asian kannalta merkityksellinen Unkarin oikeus

- 18 Tietosuoja-asetus on ollut voimassa ja sitä on pitänyt soveltaa Unkarissa 25.5.2018 alkaen. Ennakkoratkaisun saamiseksi esitetyt kysymykset ovat tulleet esiin tietosuoja-asetuksen soveltamisen osalta. **[alkup. s. 4]**

Ennakkoratkaisun tarve ja pyynnön perustelut

- 19 Ennakkoratkaisua pyytävä tuomioistuin haluaa saada Euroopan unionin tuomioistuimelta suuntaviittoa siihen, miten tietosuoja-asetuksen 5 artiklan 1 kohdan b alakohdassa tarkoitettua käyttötarkoitussidonnaisuuden periaatetta ja sen

5 artiklan 1 kohdan e alakohdassa tarkoitettua säilytyksen rajoittamista koskevaa periaatetta on tulkittava.

- 20 Asiakastiedot, jotka valittaja on tallentanut henkilötietojen tietoturvaloukkauksen kohteena olleeseen testitietokantaan, oli kerätty tilaussopimusten tekemistä varten tietosuoja-asetuksen 6 artiklan 1 kohdan b alakohdan mukaisesti, eikä vastapuoli ole riitauttanut tietojen keräämisen lainmukaisuutta.
- 21 Ennakkoratkaisua pyytävä tuomioistuin haluaa vastauksen siihen, onko tietojen keräämisen ja käsittelyn tarkoitus – jota asiassa ei ole riitautettu – muuttunut siksi, että määrättyyn tarkoitukseen kerätyt tiedot on kopioitu toiseen tietokantaan. Lisäksi se haluaa tietää, voidaanko testitietokannan perustamista (eli määrättyyn tarkoitukseen kerättyjen tietojen tallentamista toiseen sisäiseen tietojärjestelmään) ja siis tällaista asiakastietojen käsittelyn jatkamista pitää tietojen keräämisen tarkoituksen mukaisena.
- 22 Ennakkoratkaisua pyytävän tuomioistuimen mukaan käyttötarkoitussidonnaisuuden periaate ei kerro selvästi sitä, missä sisäisissä tietojärjestelmissä rekisterinpitäjällä on oikeus käsitellä laillisesti kerättyjä tietoja ja voiko se kopioida tällaiset tiedot tekstitietokantaan ilman, että sen katsottaisiin samalla muuttavan tietojen keräämisen tarkoitusta.
- 23 Siltä varalta, että testitietokannan perustamisen (eli tietojen tallentamista toiseen sisäiseen tietojärjestelmään) katsotaan olevan vastoin tietojen keräämistarkoitusta, ennakkoratkaisua pyytävä tuomioistuin haluaisi lisäksi vastauksen siihen, onko tietojen säilytysaika rajattava aikaan, joka virheiden korjaamiseen tai sopimusvelvoitteiden noudattamiseen tarvitaan.
- 24 [– –]
- 25 [kansallisia prosessioikeudellisia seikkoja]

Loppumääräykset

Budapest 21.1.2021.

[– –] [allekirjoitukset]