

Lieta C-340/21

**Lūguma sniegt prejudiciālu nolēmumu kopsavilkums saskaņā ar Tiesas
Reglamenta 98. panta 1. punktu**

Iesniegšanas datums:

2021. gada 2. jūnijs

Iesniedzējtiesa:

Varhoven administrativen sad (Bulgārija)

Datums, kurā pieņemts iesniedzējtiesas nolēmums:

2021. gada 14. maijs

Kasācijas sūdzības iesniedzēja:

VB

Atbildētājs kasācijas tiesvedībā:

Natsionalna agentsia za prihodite (Valsts ieņēmumu dienests)

Pamatlietas priekšmets

Apelācijas sūdzība par spriedumu, ar kuru kā nepamatota ir noraidīta prasība kompensēt nemantisko (nemateriālo) kaitējumu, kas esot nodarīts atbildētāja kasācijas tiesvedībā – kā [personas datu] pārziņa – prettiesiskas bezdarbības dēļ, proti, ar to, ka neesot tikuši pienācīgi izpildīti *Zakon za zashtita na lichnite danni* (Personas datu aizsardzības likums, turpmāk tekstā – “Datu aizsardzības likums”) un Regulā 2016/679 noteiktie pienākumi.

Lūguma sniegt prejudiciālu nolēmumu priekšmets un tiesiskais pamats

Lūgums sniegt prejudiciālu nolēmumu atbilstoši LESD 267. pantam par Regulas 2016/679 74., 85. un 146. apsvēruma, kā arī 4. panta 12. punkta, 5. panta 2. punkta, 24., 32. un 82. panta interpretāciju.

Prejudiciālie jautājumi

1. Vai Regulas (ES) 2016/679 24. un 32. pants ir jāinterpretē tādējādi, ka, lai varētu izdarīt pieņēmumu, ka veiktie tehniskie un organizatoriskie pasākumi nav atbilstīgi, pietiek konstatēt, ka personas datu neatļautu izpaušanu vai piekļuvi tiem Regulas (ES) 2016/679 4. panta 12. punkta izpratnē ir izdarījušas personas, kuras nav pārziņa pārvaldes darbinieki un kuras nav pakļautas tā kontrolei?
2. Ja atbilde uz pirmo jautājumu būtu noliedzoša, kādam ir jābūt tiesiskuma pārbaudes tiesā priekšmetam un apjomam, vērtējot, vai Regulas (ES) 2016/679 32. pantā minētie tehniskie un organizatoriskie pasākumi, kurus veicis pārzinis, ir atbilstīgi?
3. Ja atbilde uz pirmo jautājumu būtu noliedzoša, vai pārskatbildības princips Regulas (ES) 2016/679 5. panta 2. punkta un 24. panta – kopsakarā ar 74. apsvērumu – izpratnē ir jāinterpretē tādējādi, ka tiesvedībā atbilstoši Regulas (ES) 2016/679 82. panta 1. punktam pārzinim ir pienākums pierādīt, ka 32. pantā minētie, veiktie tehniskie un organizatoriskie pasākumi ir atbilstīgi? Vai eksperta atzinuma saņemšana ir uzskatāma par nepieciešamu un pietiekamu pierādījumu tam, lai konstatētu, vai pārziņa veiktie tehniskie un organizatoriskie pasākumi tādā situācijā kā šeit aplūkojamā bija atbilstīgi, ja neatļautā piekļuve personas datiem un to neatļautā izpaušana ir “hakeru uzbrukuma” sekas?
4. Vai Regulas (ES) 2016/679 82. panta 3. punkts ir jāinterpretē tādējādi, ka personas datu neatļautā izpaušana vai piekļuve tiem Regulas (ES) 2016/679 4. panta 12. punkta izpratnē, ko, izmantojot “hakeru uzbrukumu”, ir veikušas personas, kuras nav pārziņa pārvaldes darbinieki un kuras nav pakļautas tā kontrolei, kā tas noticis izskatāmajā lietā, ir uzskatāma par notikumu, par ko pārzinis nekādā veidā nav atbildīgs un kas attaisno tā atbrīvošanu no atbildības?
5. Vai Regulas (ES) 2016/679 82. panta 1. un 2. punkts kopsakarā ar 85. un 145. apsvērumu ir jāinterpretē tādējādi, ka tādā situācijā kā šeit aplūkojamā, kad noticis personas datu aizsardzības pārkāpums, kas izpaužas kā neatļautā piekļuve personas datiem un to neatļautā izpaušana, izmantojot “hakeru uzbrukumu”, ja šāda ļaunprātīga izmantošana nav konstatēta un/vai ja datu subjektam nav nodarīts citāds kaitējums, plaši interpretējamajā nemantiskā kaitējuma jēdzienā ietilpst – un tiesības saņemt attiecīgu kompensāciju dod – jau datu subjekta rūpes, bažas un bailes par personas datu iespējamu ļaunprātīgu izmantošanu nākotnē?

Eiropas Savienības tiesību normas un judikatūra

Eiropas Parlamenta un Padomes Regulas (ES) 2016/679 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula, turpmāk tekstā – “Regula”) 1., 4., 6., 74., 75., 76., 77., 83., 85. un 146. apsvēruma, kā arī 4. panta 2., 7. un 12. punkts, 5., 24., 32., 33., 79. un 82. pants.

Tiesas spriedums, 2013. gada 30. maijs, *Worten* (C-342/12, EU:C:2013:355), 24. un 26. punkts.

Valsts tiesību normas

Administrativnoprotsesualen kodeks (Administratīvā procesa kodekss) 144. panta 1. punkts, 203. un 208. pants.

Grazhdanski protsesualen kodeks (Civilprocesa kodekss) 154. pants.

Zakon za otgovornostta na darzhavata i obshtinite za vredi (Likums par valsts un pašvaldību atbildību par nodarīto kaitējumu) 1. pants

Zakon za zashtita na lichnite danni (Personas datu aizsardzības likums) 39. panta 1. un 2. punkts un 59. panta 1. punkts.

Īss pamatlietas faktisko apstākļu un tiesvedības izklāsts

- 1 *Natsionalna agentsia za prihodite* (Valsts ieņēmumu dienests, turpmāk tekstā – “NAP”) ir pārzinis Regulas 4. panta 7. punkta izpratnē. Saskaņā ar šīs valsts tiesību normām tas ir Finanšu ministrijas pakļautībā esoša specializēta iestāde, kuras kompetencē ir noteikt, nodrošināt un iekasēt publiskus un tiesību aktos noteiktus privātus valsts prasījumus. Izpildot tam deleģētās publiskās varas funkcijas, tas apstrādā personas datus.
- 2 2019. gada 15. jūlijā Bulgārijas plašsaziņas līdzekļi informēja visu sabiedrību, ka ir notikusi neatļauta piekļuve NAP informācijas sistēmai un ka internetā bija publiskota informācija no NAP datubāzēm, kuras ietver personas datus, kā arī informācija par nodokļiem un sociālo apdrošināšanu. Tas skāra 4 057 328 Bulgārijas pilsoņu, savukārt visu skarto datu subjektu, kas ir fiziskas personas, skaits sasniedza 6 074 140, un viņu vidū bija gan Bulgārijas pilsoņi, gan citu valstu pilsoņi. Viena no šiem datu subjektiem bija VB.
- 3 Attiecībā uz personām, kuras [esot] izdarījušas šo neatļauto piekļuvi datiem, ko plašsaziņas līdzekļi nodēvējuši par “hakeru uzbrukumu”, vēl nav pieņemts galīgs notiesājošs spriedums.
- 4 Pēc šīs [neatļautās] piekļuves datiem vairāki simti pilsoņu vērsās tiesā pret NAP ar prasību kompensēt nemantisko kaitējumu.
- 5 2019. gada 16. septembrī VB cēla *Administrativen sad Sofia-grad* (Sofijas pilsētas Administratīvā tiesa, turpmāk tekstā – “ASSG”) prasību pret NAP par kompensācijas samaksu 1000 levu (BGN) (aptuveni 511 EUR) apmērā, pamatojoties uz Regulas 82. panta 1. punktu, Likuma par valsts un pašvaldību atbildību par nodarīto kaitējumu (*Zakon za otgovornostta na darzhavata i obshtinite za vredi*) 1. panta 1. punktu un Personas datu aizsardzības likuma (*Zakon za zashtita na lichnite danni*) 39. panta 1. punktu.

- 6 Prasībā, kuru VB cēla pirmās instances tiesā notikušajā tiesvedībā, viņa apgalvoja, ka *NAP* neesot “vislabākajā veidā” izpildījusi savu pienākumu “pienācīgi nodrošināt viņas kiberdrošību” un “maksimāli iedarbīgi nodrošināt Bulgārijas Republikas pilsoņu personas datu drošību”. Tādējādi esot noticis personas datu aizsardzības pārkāpums Regulas 4. panta 12. punkta izpratnē, un personas dati esot nelikumīgi izpausti.
- 7 VB puda uzskatu, ka “nepietiekamā rūpība un iedarbīgu datu aizsardzības pasākumu nepiemērošana” liecina par *NAP* pienākuma aizsargāt pilsoņu datus neizpildi, kas uzskatāma par Regulas 24. un 32. panta pārkāpumu. Kā pārzinim *NAP* esot bijis pienākums apstrādāt personas datus tādā veidā, kas “lai tiktu nodrošināta atbilstoša [...] drošība”, īstenojot atbilstīgus tehniskos un organizatoriskos pasākumus.
- 8 VB apgalvoja, ka *NAP* pienākumu neizpildes rezultātā viņai esot nodarīts nemantisks kaitējums, kas izpaužas kā uztraukums un bažas par viņas personas datu turpmāku ļaunprātīgu izmantošanu, piemēram, tādā veidā, ka viņai tiktu atņemts viņas īpašums, ļaunprātīgi izmantoti viņas konti bankās, viņas vārdā tiktu noslēgti kredīta līgumi, veiktas izmaiņas viņas ģimenes stāvoklī vai nozagta viņas identitāte. Viņa puda sašutumu par “apjomīgo ielaušanos *NAP* informācijas sistēmā” un norādīja, ka jūtas tā, ka valsts viņu neaizsargā. Viņai esot bailes, ka no viņas tikšot izspiesta nauda, viņai uzbruks vai viņa tikšot nolaupīta.
- 9 *NAP* uzskatīja, ka prasība ir nepamatota. VB neesot pieprasījusi no *NAP* konkrētu informāciju par to, kādus personas datus ir skārusi minētā piekļuve.
- 10 Pēc notikušās piekļuves *NAP* nekavējoties esot veicis pasākumus, lai aizsargātu pilsoņu tiesības un intereses. Esot notikušas tikšanās ar drošības dienestu, *Notarialna kamara* (Notāru padome), *Agentsia po vpisvaniata* (Reģistru aģentūra), *Asotsiatsia na targovskite banki* (Komercbanku asociācija) u.c. pārstāvjiem un ekspertiem, lai koordinētu šīs piekļuves seku ierobežošanas pasākumus. *NAP* tīmekļvietnē esot izveidotas īpašas sadaļas par šo kiberuzbrukumu, kurās esot publicēta jaunākā informācija.
- 11 *NAP* uzskata, ka trūkst cēloņsakarības starp apgalvoto nemantisko kaitējumu un neatļauto piekļuvi personas datiem. *NAP* esot tāda apzināta uzbrukuma upuris, ko īstenojušas trešās personas, nevis *NAP* darbinieki. Tādēļ *NAP* neesot atbildīgs par nodarīto kaitējumu.
- 12 *NAP* apgalvoja, ka esot veicis daudzus pasākumus. Proti, tas esot ieviesis procesu vadības sistēmas un informācijas drošības vadības sistēmas, apstiprinājis procedūras, kuras atbilst starptautiskajiem kvalitātes standartiem ISO 9000 un ISO 9001, kā arī piemērojis informācijas drošības vadības politiku, noteikumus, procedūras, instrukcijas un metodes.
- 13 *NAP* iesniedza pierādījumus, proti, dažādus iekšējos dokumentus par laikposmu no 2013. gada janvāra līdz 2019. gada maijam attiecībā uz datubāzu saturu, izveides procedūru, uzturēšanu un piekļuvi; informācijas drošības vadības sistēmu

ieviešanu; prevencijas procedūru; iekšējiem noteikumiem par tīkla un informācijas drošību; instrukcijām par informācijas apstrādi; personas datu aizsardzības politiku; personas datu aizsardzības pasākumiem un līdzekļiem, kā arī risku novērtēšanas metodēm un procedūru.

- 14 ASSG ar 2020. gada 27. novembra spriedumu noraidīja VB prasību kā nepamatotu.
- 15 ASSG norādīja, ka neatļautā piekļuve NAP datubāzei esot notikusi, izmantojot “hakeru uzbrukumu”, ko īstenojušas personas, pret kurām esot uzsākta kriminālizmeklēšana, kas vēl neesot pabeigta.
- 16 Prettiesiskais rezultāts neļaujot prezumēt, ka pārzinis nav izpildījis savu pienākumu īstenot atbilstīgus tehniskos un organizatoriskos pasākumus datubāzes aizsardzības nodrošināšanai, lai neviens nekādā veidā un ne ar kādiem līdzekļiem nevarētu piekļūt šai datubāzei.
- 17 ASSG pauda uzskatu, ka prasītājam esot jānorāda, kādas (tehniskas) darbības NAP būtu bijis jāveic, taču faktiski tas nav veicis vai ir veicis slikti, kā rezultātā ir notikusi neatļauta piekļuve personas datiem un to neatļauta izpaušana vai kas ir sekmējis šāda rezultāta iestāšanos.
- 18 ASSG pauda uzskatu, ka, ņemot vērā iesniegtos pierādījumus, nav konstatējama pārziņa bezdarbība. VB neesot nodarīts atlīdzināms nemantisks kaitējums. Piedzīvotā psiholoģiskā spriedze, ko izraisīja ziņa par neatļauto piekļuvi NAP informācijas datubāzēm, esot normāla reakcija, tomēr tas neesot faktiski nodarīts kaitējums juridiskā izpratnē. VB neesot interesējies par to, kurus viņas personas datus ir konkrēti skārusi minētā piekļuve. Šāda rīcība neliecinot par spēcīgu emocionālu spriedzi.
- 19 ASSG nosprieda, ka publiskais paziņojums par notikušo nelikumīgo piekļuvi NAP datubāzei nav ietekmējis VB dzīvi, proti, viņas pašapziņu, pašvērtējumu, darbu, attiecībām un veselības stāvokli. Nepastāvot cēloņsakarība ar piedzīvotajām negatīvajām emocijām, jo tās neesot NAP rīcības rezultāts.
- 20 VB šo ASSG spriedumu pārsūdzēja iesniedzējtiesā – *Varhoven administrativen sad* (Augstākā administratīvā tiesa, turpmāk tekstā – “VAS”).

Pamatlietas pušu galvenie argumenti

- 21 Kasācijas sūdzībā VB apgalvo, ka ASSG esot nepareizi sadalījusi pierādīšanas pienākumu attiecībā uz to, kā ir pierādāms negatīvs fakts – pārziņa bezdarbība, proti, atbilstīgu tehnisko un organizatorisko pasākumu neveikšana.
- 22 VB uzskata, ka iedarbīgu pasākumu piemērošana ietilpst NAP rīcības brīvībā, tādēļ viņai neesot iespējams izklāstīt, kādi konkrēti pienākumi NAP personālam

būtu bijuši jāizpilda, taču faktiski nav izpildīti. *NAP* iesniegtie pierādījumi neesot apliecinājuši, ka veiktie tehniskie un organizatoriskie pasākumi būtu atbilstīgi.

- 23 *VB* apgalvo, ka uztraukums par personas datu iespējamu turpmāku ļaunprātīgu izmantošanu esot uzskatāms nevis par hipotētisku, bet gan par faktisku nemantisku kaitējumu, kas esot jākompensē. Parasts nemantisks kaitējums neesot jāpierāda.
- 24 *NAP* apgalvo, ka *ASSG* esot pamatoti izdarījusi pieņēmumu, ka *NAP* kā pārzinis nav bijis bezdarbīgs, bet gan ir veicis daudzus tehniskus un organizatoriskus pasākumus personas datu aizsardzībai to apstrādē. Kaitējuma faktiska iestāšanās neesot pierādīta. Uztraukums un bailes par notikumiem nākotnē neesot jākompensē.

Īss lūguma sniegt prejudiciālu nolēmumu pamatojuma izklāsts

- 25 Līdzīgas pirmās instances tiesvedības pret *NAP* ir beigušās ar pretrunīgiem rezultātiem. Prasības ir noraidītas kā nepamatotas vai apmierinātas daļēji vai pilnā apmērā. Tiesību akti attiecībā uz visiem pārziņa atbildības elementiem ir interpretēti un piemēroti pretrunīgi.
- 26 *VAS* uzskata, ka Regulas 82. pantā paredzētās atbildības piemērojamības nosacījumi ietver: i) pārziņa izdarītu šīs regulas pārkāpumu; ii) mantisku vai nemantisku kaitējumu, kas nodarīts datu subjektam, un iii) cēloņsakarību starp nodarīto kaitējumu un konkrēto pārkāpumu.

Pirmais jautājums

- 27 Saskaņā ar Regulas 24. panta 1. punktu pārzinis īsteno atbilstīgus tehniskos un organizatoriskos pasākumus, lai nodrošinātu un spētu uzskatāmi parādīt, ka apstrāde notiek atbilstoši šai regulai. Ja nepieciešams, minētos pasākumus pārskata un atjaunina.
- 28 Regulas 32. pantā ir paredzēti pārziņa pienākumi saistībā ar apstrādes drošību, kuri ir nozīmīgi 24. pantā paredzētajai atbildībai un kuri to izraisa, turklāt ir uzskaitīti kritēriji, pēc kuriem ir piemērojami atbilstīgie tehniskie un organizatoriskie pasākumi, lai nodrošinātu tādu drošības līmeni, kas atbilst riskam. Pie tiem pieder “tehniskās iespējas, īstenošanas izmaksas, apstrādes veids, apmērs, konteksts un nolūki, kā arī dažādas iespējamības un nopietnības pakāpes riski attiecībā uz fizisku personu tiesībām un brīvībām”.
- 29 Regulā nav sniegta jēdziena “atbilstīgi tehniskie un organizatoriskie pasākumi” definīcija. 74. apsvērumā ir norādīts, ka pārzinim ir jāīsteno atbilstīgi un iedarbīgi pasākumi un ka tam vajadzētu spēst parādīt, ka apstrādes darbības notiek atbilstoši šai regulai un ka pasākumi ir arī iedarbīgi.

- 30 No iepriekš minētā var secināt, ka pārzinim ir jāveic risku novērtējums pēc Regulas 32. pantā noteiktajiem kritērijiem un ka, balstoties uz šo novērtējumu, viņam ir jāveic tehniski un organizatoriski pasākumi, kas ir atbilstīgi un ar kuriem ir iespējams attiecībā uz personas datiem nodrošināt nepieciešamo drošības līmeni atbilstoši riskam. Ieviešot atbilstīgus tehniskos un organizatoriskos pasākumus, pārzinis nodrošina, ka personas datu apstrāde notiek atbilstoši Regulai.
- 31 No minētajiem tiesību aktiem izriet, ka atbilstīgu tehnisko un organizatorisko pasākumu izvēle ir to lietderīguma jautājums. Tomēr pārziņa veiktais lietderīguma novērtējums nav pakļauts pārbaudei tiesā, jo tiesa pārbauda tiesiskumu. Vienlaikus personas datu apstrādei, izmantojot esošo rīcības brīvību tehnisko un organizatorisko pasākumu izvēles ziņā, ir jānotiek, ievērojot Regulu un izvirzīto mērķi ievērot fizisku personu pamattiesības uz personas datu aizsardzību.
- 32 Ņemot vērā visu iepriekš izklāstīto, VAS vēlas noskaidrot, vai Regulas 24. un 32. pants ir jāinterpretē tādējādi, ka jau tāda pretiesiska rezultāta iestāšanās, kas izpaužas kā personas datu neatļauta izpaušana vai piekļuve tiem Regulas 4. panta 12. punkta izpratnē, pati par sevi pierāda, ka pārziņa veiktie tehniskie un organizatoriskie pasākumi nebija atbilstīgi.

Otrais jautājums (ja atbilde uz pirmo jautājumu būtu noliedzoša)

- 33 Tā kā tehnisko un organizatorisko pasākumu izvēle un piemērošana ir atstāta pārziņa subjektīvā vērtējuma ziņā un ietilpst viņa rīcības brīvības jomā, VAS rodas jautājums, kādam ir jābūt tiesiskuma pārbaudes tiesā priekšmetam un apjomam, vērtējot, vai pārziņa veiktie tehniskie un organizatoriskie pasākumi ir atbilstīgi un atbilst Regulas 24. un 32. pantam.
- 34 VAS šaubās, vai ir pietiekami, ja tiesa konstatē, kādā veidā pārzinis ir izpildījis pienākumus, kas noteikti minētajās tiesību normās, vai tomēr tiesai pēc būtības ir jāizvērtē veiktie un īstenotie tehniskie un organizatoriskie pasākumi, kuri Regulā tomēr ir minēti tikai piemēru veidā un kuri tiek īstenoti atkarībā no to lietderības.

Trešais jautājums (ja atbilde uz pirmo jautājumu būtu noliedzoša)

- 35 Saskaņā ar Regulas 5. panta 2. punktu pārzinis ir atbildīgs par to, ka tiek ievērotas tās pašas normas 1. punktā minētie principi, kas attiecas uz personas datu apstrādi, un pārzinim ir jāspēj šādu atbilstību pierādīt. Regulas 24. panta 1. punktā ir noteikts pārziņa pienākums "īsteno[t] atbilst[īg]us tehniskus un organizatoriskus pasākumus, lai nodrošinātu un spētu uzskatāmi parādīt, ka apstrāde notiek saskaņā ar šo regulu".
- 36 Regulas 82. panta 3. punkts pieļauj, ka pārzinis vai apstrādātājs tiek atbrīvots no otrajā punktā paredzētās atbildības, "ja tas pierāda, ka nekādā veidā nav atbildīgs par notikumu, ar ko nodarīts attiecīgais kaitējums". Saskaņā ar iepriekš minēto

2. punktu pārzinis ir atbildīgs par kaitējumu, kas nodarīts ar apstrādi, kura neatbilst Regulai.

- 37 Saskaņā ar valsts tiesību normām ikvienam lietas dalībniekam tiesvedībā ir pienākums pierādīt faktus, uz kuriem tas balsta savus prasījumus vai iebildumus. Līdzīgās tiesvedībās pirmās instances tiesas šo pierādīšanas pienākumu ir atšķirīgi sadalījušas starp prasītāju un atbildētāju.
- 38 Izskatāmajā lietā nozīmīgs ir jautājums, vai pārskatatbildības princips, kas izriet no Regulas 5. panta 2. punkta kopsakarā ar tās 74. apsvērumu un 24. panta 1. punktu, ir jāinterpretē tādējādi, ka attiecīgās tiesību normas apvērš pierādīšanas pienākumu un ka pārzinim, pret kuru celta prasība samaksāt kompensāciju par Regulas pārkāpumu, ir jāpierāda, ka viņa piemērotie tehniskie un organizatoriskie pasākumi ir atbilstīgi.
- 39 Līdztekus jautājumam par pārbaudes tiesā priekšmetu un apjomu, izvērtējot no Regulas izrietošo pienākumu izpildi, problemātisks ir arī jautājums, kā un, balstoties uz kādiem pierādījumiem, ir jāpārbauda, vai šie pienākumi tika izpildīti un, it īpaši tas, vai tika piemēroti visi atbilstīgie tehniskie un organizatoriskie pasākumi.
- 40 Tiesvedības laikā *NAP* iesniedza pierādījumus par informācijas tīklu aizsardzības nodrošināšanu atbilstoši dokumentos norādītajiem standartiem, tomēr netika iegūts tehniskās ekspertīzes atzinums, kurā būtu konstatēts, vai tehniskie un organizatoriskie pasākumi bija atbilstīgi Regulas izpratnē. VAS apzinās, ka tādām pārzinim kā *NAP* ir pienākums tīklu un informācijas drošības nolūkā piemērot organizatoriskus, tehnoloģiskus un tehniskus pasākumus, kas ir samērīgi ar kibernetizācijas radīto apdraudējumu, lai līdz minimumam samazinātu šāda apdraudējuma īstenošanās risku. Tomēr tehnisko ekspertu piekļuve datiem ikvienā tiesvedībā, kuras tiesiskais pamats ir Regulas 82. pants, varētu nozīmēt jaunas negatīvas sekas attiecībā uz personas datu aizsardzību.
- 41 Ņemot vērā tehniskās iespējas, esošos informācijas tīklu sistēmu aizsardzības standartus un notikušo neatļauto piekļuvi, izmantojot “hakeru uzbrukumu”, ko īstenoja personas, kuras nav pārziņa pārvaldes darbinieki, VAS rodas jautājums, vai tiesas uzdotas tehniskās ekspertīzes atzinuma saņemšanu var uzskatīt par nepieciešamu un pietiekamu pierādījumu tam, lai konstatētu, vai veiktie un piemērotie tehniskie un organizatoriskie pasākumi bija atbilstīgi un tādi, ar kuriem iespējams nodrošināt personas datu aizsardzību.

Ceturtais jautājums

- 42 Būdam apstrādē iesaistīts pārzinis, *NAP* ir atbildīgs kaitējuma gadījumā, tomēr saskaņā ar 82. panta 3. punktu var tikt atbrīvots no atbildības, ja tas pierāda, ka nekādā veidā nav atbildīgs par notikumu, ar ko nodarīts attiecīgais kaitējums.

- 43 Šajā lietā nav strīda par to, ka piekļuve personas datiem notika, izmantojot pret NAP vērstu "hakeru uzbrukumu". Neatļautā piekļuve personas datiem un to neatļauta izpaušana nenotika, NAP darbiniekiem veicot personas datu apstrādi vai saistībā ar to.
- 44 VAS lūdz konstatēt, vai izskatāmajā lietā ir iespējams izdarīt pieņemumu, ka tas ir notikums, par kuru pārzinis nekādā ziņā nav atbildīgs, un, ka atbilstoši tam šis apstāklis to atbrīvo no atbildības.

Piektais jautājums

- 45 Datu subjekts prasa kompensēt nemantisko kaitējumu, kas izpaužas kā uztraukums, bailes, spriedze, nedrošības sajūta un bažas par turpmāku viņas personas datu ļaunprātīgu izmantošanu dažādos veidos, kā viņa to ir norādījusi. Nekas neliecina par to, ka VB personas dati būtu ļaunprātīgi izmantoti.
- 46 Kā izriet no Regulas 75. un 85. apsvēruma, mantiskā un nemantiskā kaitējuma piemēru uzskaitījumā ir ņemti vērā personas datu veidi un nelabvēlīgā ietekme uz datu subjektu, nevis tikai datu subjekta subjektīvās sajūtas.
- 47 Regulas 146. apsvērumā ir noteikta atbildības robeža. Atbildība iestājas par "kaitējumu", kas personai nodarīts tādas apstrādes rezultātā, ar kuru ir pārkāpta Regula.
- 48 Pēc tam, kad jau ir notikusi piekļuve datiem, datu subjekta personas dati var kļūt par daudzu tādu mantiska un nemantiska rakstura ļaunprātīgas izmantošanas gadījumu objektu, kuri izraisa ievērojamas sekas. Plašai sabiedrībai ir zināmi šādi ļaunprātīgas izmantošanas gadījumi, un tas var būt par iemeslu to datu subjektu lielākam uztraukumam, kurus ir skāris "hakeru uzbrukums". Izskatāmajā lietā turpmāka ļaunprātīga izmantošana (tā kā trūkst informācijas par jau notikušu ļaunprātīgu izmantošanu) ir tikai pieņemums, hipotēze par iespējamu, bet neskaidru risku attiecībā uz datu subjekta tiesībām.
- 49 Iepriekš izklāstīto apsvērumu dēļ rodas jautājums, vai datu subjekta negatīvas sajūtas šajā kontekstā, tas ir, vai fakts, ka tikai ir radies personas datu iespējamās turpmākas ļaunprātīgas izmantošanas risks, ietilpst nemantiskā kaitējuma jēdzienā, kas ir plaši interpretējams, un vai tas ir uzskatāms par iemeslu kompensācijas saņemšanai atbilstoši Regulas 82. panta 1. punktam kopsakarā ar 146. apsvērumu.
- 50 Tomēr ir iespējams, ka Regulas 82. panta 1. punktu kopsakarā ar 146. apsvērumu nevar interpretēt tādējādi, ka jebkādas datu subjekta negatīvas sajūtas, bailes vai uztraukums dotu tiesības saņemt kompensāciju par nemantisku kaitējumu, ja pirms tam nav notikusi nelikumīga personas datu izmantošana, piemēram, atņemts īpašums, datu subjekta vārdā noslēgts kredīta līgums vai nozagta datu subjekta identitāte.