Kohtuasi C-340/21

Eelotsusetaotluse kokkuvõte vastavalt Euroopa Kohtu kodukorra artikli 98 lõikele 1

Saabumise kuupäev:

2. juuni 2021

Eelotsusetaotluse esitanud kohus:

Varhoven administrativen sad (Bulgaaria kõrgeim halduskohus)

Eelotsusetaotluse kuupäev:

14. mai 2021

Kassaator:

VB

Vastustaja kassatsioonimenetluses:

Natsionalna agentsia za prihodite (riigi maksuamet)

Põhikohtuasja ese

Kassatsioonkaebus kohtuotsuse peale, millega jäeti põhjendamatuse tõttu rahuldamata nõue hüvitada mittemateriaalne kahju, mis tekkis seetõttu, et vastustaja kassatsioonimenetluses kui vastutav töötleja jättis õigusvastaselt täitmata oma kohustused, mis tulenesid isikuandmete kaitse seadusest (Zakon za zashtita na lichnite danni; edaspidi „andmekaitseseadus“) ja määrusest 2016/679.

Eelotsusetaotluse ese ja õiguslik alus

ELTL artikli 267 alusel esitatud eelotsusetaotlus, millega palutakse tõlgendada määruse 2016/679 põhjendusi 74, 85 ja 146 ning artikli 4 punkti 12, artikli 5 lõiget 2, artikleid 24, 32 ja 82.

Eelotsuse küsimused

1. Kas määruse (EL) 2016/679 artikleid 24 ja 32 tuleb tõlgendada nii, et võetud tehniliste ja korralduslike meetmete mitteasjakohasuse eeldamiseks piisab sellest,

et isikuandmete loata avalikustamine või neile juurdepääs määruse (EL) 2016/679 artikli 4 punkti 12 tähenduses on põhjustatud isikute poolt, kes ei ole vastutava töötleja administratsiooni töötajad ning ei allu tema kontrollile?

2. Juhul, kui vastus esimesele küsimusele on eitav, milline peab olema õiguspärasuse kohtuliku kontrolli ese ja ulatus hindamaks, kas vastutava töötleja võetud tehnilised ja korralduslikud meetmed on määruse (EL) 2016/679 artikli 32 kohaselt asjakohased?

3. Juhul, kui vastus esimesele küsimusele on eitav, kas vastutuse põhimõtet, mis on sätestatud määruse (EL) 2016/679 artikli 5 lõikes 2 ja artiklis 24 koostoimes põhjendusega 74, tuleb tõlgendada nii, et määruse (EL) 2016/679 artikli 82 lõike 1 kohases kaebemenetluses lasub vastutaval töötlejal kohustus tõendada, et määruse artikli 32 kohaselt võetud tehnilised ja korralduslikud meetmed on asjakohased? Kas eksperdiarvamuse küsimist võib pidada vajalikuks ja piisavaks tõendiks, et tuvastada, kas vastutava töötleja võetud tehnilised ja korralduslikud meetmed olid asjakohased niisugusel juhul nagu käesolevas asjas, mil isikuandmetele loata juurdepääs ja nende avalikustamine toimus nn häkkerite rünnaku tagajärjel?

4. Kas määruse (EL) 2016/679 artikli 82 lõiget 3 tuleb tõlgendada nii, et isikuandmete loata avalikustamine või neile juurdepääs määruse (EL) 2016/679 artikli 4 punkti 12 tähenduses, mille – nagu käesoleval juhul – oli põhjustanud nn häkkerite rünnak, mille korraldasid isikud, kes ei ole vastutava töötleja administratsiooni töötajad ega allu tema kontrollile, kujutab endast asjaolu, mille eest ei ole vastutav töötleja mingil viisil vastutav ja mis annab õiguse vastutusest vabastamiseks?

5. Kas määruse (EL) 2016/679 artikli 82 lõikeid 1 ja 2 koostoimes põhjendustega 85 ja 146 tuleb tõlgendada nii, et niisugusel juhul nagu käesolevas asjas, mil isikuandmete kaitse rikkumine seisnes isikuandmetele loata juurdepääsus ja nende levitamises nn häkkerite rünnaku tagajärjel, kuuluvad üksnes andmesubjekti kogetud mure, kartus ja hirm isikuandmete võimaliku tulevase kuritarvitamise pärast mittemateriaalse kahju laialt tõlgendatava mõiste alla ning annavad õiguse nõuda kahju hüvitamist, kui niisugust kuritarvitust ei ole tuvastatud ja/või andmesubjektile ei ole tekkinud muud kahju?

Euroopa Liidu õigusnormid ja kohtupraktika

Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta määrus (EL) 2016/679 füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus; edaspidi „määrus“): põhjendused 1, 4, 6, 74, 75, 76, 77, 83, 85, 146, artikli 4 punktid 2, 7 ja 12, artiklid 5, 24, 32, 33, 79, 82.

Euroopa Kohtu 30. mai 2013. aasta otsus kohtuasjas Worten (C-342/12; EU:C:2013:355), punktid 24 ja 26.

Liikmesriigi õigusnormid

Haldusmenetluse seadustik (Administrativnoprotsesualen kodeks) – artikli 144 lõige 1, artiklid 203 ja 208.

Tsiviilkohtumenetluse seadustik (Grazhdanski protsesualen kodeks) – artikkel 154.

Riigi ja kohaliku omavalitsuse vastutuse seadus (Zakon za otgovornostta na darzhavata i obshtinite za vredi) – artikkel 1.

Isikuandmete kaitse seadus (Zakon za zashtita na lichnite danni) – artikli 39 lõiked 1 ja 2, artikli 59 lõige 1.

Kohtuasja asjaolude ja menetluse lühikokkuvõte

1 Natsionalna agentsia za prihodite (riigi maksuamet; edaspidi „NAP“) on vastutav töötleja määruse artikli 4 punkti 7 tähenduses. Liikmesriigi õiguse kohaselt allub see spetsialiseerunud haldusasutus rahandusministrile ja tema pädevusse kuulub avalik-õiguslike ning seadusega sätestatud eraõiguslike riigi nõuete tuvastamine, tagamine ja sissenõudmine. Talle delegeeritud avalik-õiguslike volituste täitmisel töötleb NAP isikuandmeid.

2 15. juulil 2019. aastal teavitas Bulgaaria meedia avalikkust, et NAPi infosüsteemile on saadud loata juurdepääs ning et info selle andmebaasidest, mis sisaldasid isikuandmeid ning maksu- ja sotsiaalkindlustusalast teavet, on Internetis avalikustatud. Kõnealune leke puudutas 4 057 328 Bulgaaria kodanikku, ning kõigi puudutatud füüsiliste isikute arv, kelle hulka kuulusid nii Bulgaaria kui ka välisriikide kodanikud, ulatus 6 074 140 isikuni. Puudutatud andmesubjektide hulka kuulub ka VB.

3 Kuni praeguse ajani ei ole isikute suhtes, kes isikuandmetele loata juurde pääsesid, ehk panid meedia sõnul [väidetavalt] toime häkkerite rünnaku, tehtud lõplikku süüdimõistvat kohtuotsust.

4 Pärast isikuandmetele loata juurdepääsu intsidenti nõudsid sajad kodanikud NAPilt mittemateriaalse kahju hüvitamist.

5 16. septembril 2019. aastal esitas VB Administrativen sad Sofia-grad’i (Sofia halduskohus; edaspidi „ASSG“) määruse artikli 82 lõike 1, riigi ja kohaliku omavalitsuse vastutuse seaduse (Zakon za otgovornostta na darzhavata i obshtinite za vredi) artikli 1 lõike 1 ning isikuandmete kaitse seaduse (Zakon za zashtita na lichnite danni) artikli 39 lõike 1 alusel NAPi vastu kahju hüvitamise nõude summas 1000 leevi (ligikaudu 511 eurot).

6 Esimese astme kohtu menetluses esitatud nõudes väitis VB, et NAP ei ole „parimal moel“ täitnud oma kohustust „tagada laitmatult tema küberturvalisus“

ning „tagada tõhusalt kõige kõrgemal tasemel Bulgaaria Vabariigi kodanike isikuandmete turvalisus“. Seetõttu toimus isikuandmetega seotud rikkumine määruse artikli 4 punkti 12 tähenduses ning leidis aset isikuandmete ebaseaduslik avaldamine.

7 VB oli seisukohal, et „hooletuse ja tõhusate andmekaitsemeetmete kasutamata jätmise“ näol on NAP jätnud täitmata oma kohustuse kodanike andmeid kaitsta ning et see kujutab endast määruse artiklite 24 ja 32 rikkumist. Vastutava töötlejana on NAP kohustatud töötlema isikuandmeid viisil, mis „tagab asjakohase turvalisuse“, rakendades asjakohaseid tehnilisi ja korralduslikke meetmeid.

8 VB väitis, et NAPi kohustuse rikkumise tõttu on talle tekkinud mittemateriaalne kahju, mis väljendub mures ja kartuses tema isikuandmete tulevase kuritarvitamise pärast, näiteks sel moel, et ta võib oma varast ilma jääda, tema pangakontosid kuritarvitatakse, tema nimel sõlmitakse laenulepinguid, tema perekonnaseisu muudetakse või pannakse toime identiteedivargus. Ta on „suure sissemurdmise tõttu NAPi infosüsteemi“ äärmiselt nördinud ning tunneb, et riik ei kaitse teda. Tal on hirm, et temalt hakatakse välja pressima, et teda rünnatakse või ta röövitakse.

9 NAP leiab, et nõue on põhjendamatu. VB ei ole NAPilt küsinud mingit infot selle kohta, millistele konkreetsetele isikuandmetele loata juurde pääseti.

10 Pärast loata juurdepääsu võttis NAP viivitamatult meetmed kodanike õiguste ja huvide kaitseks. Toimusid kohtumised julgeolekuasutuste, Notarialna kamara (notarite koja), Agentsia po vpisvaniata (registrite agentuuri), Asotsiatsia na targovskite banki (kommertspankade liidu) jt esindajate ja ekspertidega, et kooskõlastada meetmeid loata juurdepääsu tagajärgede piiramiseks. NAPi veebilehele loodi spetsiaalsed küberrünnakut puudutavad alljaotised, milles avaldati päevakohast infot.

11 NAPi hinnangul puudub väidetava mittemateriaalse kahju ja isikuandmetele loata juurdepääsu vahel põhjuslik seos. NAP on langenud kolmandate isikute korraldatud tahtliku rünnaku ohvriks, kusjuures need isikud ei ole tema töötajad. Seetõttu ei ole ta tekkinud kahju eest vastutav.

12 NAP väitis, et ta on võtnud rea meetmeid. Konkreetselt on ta sisse seadnud protsesside haldamise süsteemid ja infoturbe haldamise süsteemid, kiitnud heaks menetlused, mis vastavad rahvusvahelistele kvaliteedistandarditele ISO 9000 ja ISO 9001, ta rakendab infoturbe haldamise juhiseid, reegleid, menetlusi, juhendeid ja meetodeid.

13 NAP esitas tõendid, milleks olid 2013. aasta jaanuarist kuni 2019. aasta maini koostatud erinevad asutusesisesed dokumendid andmebaaside sisu, nende loomise menetluse, nende haldamise ja neile juurdepääsu kohta; samuti esitati dokumendid infoturbe haldamise rakendamise ning preventsioonimenetluse kohta; asutusesisesed juhised võrgu- ja infoturbe kohta; juhendid informatsiooni

käsitlemise kohta; juhised isikuandmete kaitse kohta; isikuandmete kaitse meetmed ja vahendid; riskianalüüsi meetodid ja menetlused.

14 ASSG jättis 27. novembri 2020. aasta otsusega VB kaebuse põhjendamatuse tõttu rahuldamata.

15 ASSG märkis, et NAPi andmebaasile said häkkerite rünnaku tagajärjel loata juurdepääsu isikud, kelle suhtes on alustatud uurimist, mis ei ole veel lõpetatud.

16 Ebaseaduslik tulemus ei luba eeldada, et vastutav töötleja on jätnud täitmata oma kohustused võtta andmebaaside kaitse tagamiseks asjakohaseid tehnilisi ja korralduslikke meetmeid, et mitte keegi ei saaks mis tahes viisil ja vahenditega kunagi sellele andmebaasile juurdepääsu.

17 ASSG leidis, et kaebaja peab näitama, milliseid (tehnilisi) toiminguid oleks NAP pidanud tegelikult tegema, kuid jättis tegemata või tegi halvasti, mistõttu oli tulemuseks loata juurdepääs isikuandmetele ja nende avaldamine, või mis aitasid kaasa sellise tagajärje tekkimisele.

18 ASSG hinnangul ei olnud esitatud tõendite põhjal võimalik vastutava töötleja rikkumist tuvastada. VBle ei ole tekkinud mittemateriaalset kahju, mille hüvitamist on tal õigus nõuda. Kogetud emotsionaalne surve, mis tekkis NAPi andmebaasidesse loata juurdepääsu uudise tõttu, on normaalne, kuid ei kujuta endast tegelikult tekkinud kahju õiguslikus tähenduses. VB ei ole tundnud huvi, konkreetselt millistele tema isikuandmetele loata juurde pääseti. Niisugune käitumine ei väljenda tugevat emotsionaalset stressi.

19 ASSG leidis, et NAPi andmebaasile saadud ebaseadusliku juurdepääsu avalikustamine ei ole mõjutanud VB elu tema eneseteadvuse, enesetunde, töö, suhete ning tervisliku seisundi aspektidest. Puudub põhjuslik seos läbi elatud negatiivsete emotsioonidega, sest need ei ole NAPi tegevuse tulemus.

20 VB vaidlustas ASSG otsuse eelotsusetaotluse esitanud kohtus, Varhoven administrativen sad'is (kõrgeim halduskohus, edaspidi „VAS“).

Põhikohtuasja poolte peamised argumendid

21 Kassatsioonkaebuses väidab VB, et seoses negatiivse asjaolu tõendamisega, ehk selles osas, et vastutav töötleja on jätnud täitmata oma kohustuse võtta asjakohased tehnilised ja korralduslikud meetmed, on ASSG jaotanud tõendamiskoormise vääralt.

22 VB on seisukohal, et tõhusate meetmete rakendamine on NAPi pädevuses, mistõttu ei ole võimalik näidata, milliseid konkreetseid kohustusi oleks NAPi töötajad pidanud täitma, kuid jätsid siiski täitmata. NAPi esitatud dokumendid ei ole suutnud tõendada, et võetud tehnilised ja korralduslikud meetmed olid asjakohased.

23 VB väidab, et mure isikuandmete võimaliku tulevase kuritarvitamise pärast kujutab endast mitte hüpoteetilist, vaid tegelikku mittemateriaalset kahju, mis tuleb hüvitada. Tavapärase mittemateriaalse kahju tekkimist ei pea tõendama.

24 NAP leiab, et ASSG lähtus õigesti sellest, et vastutava töötlejana ei ole ta midagi tegemata jätnud, vaid võtnud rea tehnilisi ja korralduslikke meetmeid isikuandmete töötlemise kaitseks. Kahju tegelik tekkimine ei ole tõendatud. Muret ja hirmu tulevaste sündmuste pärast ei pea hüvitama.

Eelotsusetaotluse põhjenduste lühikokkuvõte

25 Sarnased NAPi suhtes algatatud kohtumenetlused lõppesid esimeses kohtuastmes vastuoluliste tulemustega. Kaebused jäeti põhjendamatuse tõttu rahuldamata või hoopis rahuldati need täielikult või osaliselt. Vastutava töötleja vastutuse kõigi elementide suhtes tõlgendati ja kohaldati õigusnorme vastuoluliselt.

26 VAS on seisukohal, et määruse artikli 82 kohane vastutuse teokoosseis hõlmab järgmist: i) määruse rikkumine vastutava töötleja poolt; ii) andmesubjektile tekkinud materiaalne või mittemateriaalne kahju, ja iii) tekkinud kahju ja konkreetse rikkumise vaheline põhjuslik seos.

Esimene küsimus

27 Määruse artikli 24 lõike 1 kohaselt rakendab vastutav töötleja asjakohaseid tehnilisi ja korralduslikke meetmeid, et tagada ja suuta tõendada isikuandmete töötlemist kooskõlas käesoleva määrusega. Vajaduse korral vaadatakse need meetmed läbi ja ajakohastatakse neid.

28 Määruse artikkel 32 näeb ette vastutava töötleja kohustused seoses töötlemise turvalisusega, mis on olulised vastutava töötleja artikli 24 järgse vastutuse mõttes ning on selle vastutuse tekkimise aluseks; seejuures loetletakse artiklis kriteeriumid, mille põhjal tuleb asjakohaseid tehnilisi ja korralduslikke meetmeid kohaldada, et tagada ohule vastav turvalisuse tase. Kõnealuste kriteeriumide hulka kuuluvad „teaduse ja tehnoloogia viimane areng, rakendamise kulud, isikuandmete töötlemise laad, ulatus, kontekst ja eesmärgid, ning erineva tõenäosuse ja suurusega ohud füüsiliste isikute õigustele ja vabadustele“.

29 Määrus ei defineeri mõistet „asjakohased tehnilised ja korralduslikud meetmed“. Põhjenduses 74 on märgitud, et vastutav töötleja on kohustatud rakendama asjakohaseid ja tõhusaid meetmeid ning olema võimeline tõendama isikuandmete töötlemise toimingute kooskõla määrusega, sealhulgas meetmete tõhusust.

30 Eeltoodu võimaldab järeldada, et vastutav töötleja peab läbi viima ohuhindamise vastavalt määruse artiklis 32 sätestatud kriteeriumidele, mille alusel peab ta võtma asjakohased tehnilised ja korralduslikud meetmed, mis tagavad vajadust ja ohule vastavust arvesse võttes isikuandmetele asjakohase turvalisuse taseme.

Asjakohaste tehniliste ja korralduslike meetmete rakendamisega tagab vastutav töötleja, et ta töötleb isikuandmeid kooskõlas määrusega.

31 Eeltoodud õigusnormidest tuleb, et asjakohaste tehniliste ja korralduslike meetmete valik peab lähtuma eesmärgipärasusest. Seda, kuidas vastutav töötleja on eesmärgipärasust hinnanud, ei saa aga kohtulikult kontrollida, sest kohus hindab õiguspärasust. Samas peab isikuandmete töötlemine tehniliste ja korralduslike meetmete valiku osas eksisteeriva kaalutlusõiguse raames toimuma määruse piirides ning järgides eesmärki tagada füüsiliste isikute põhiõigus isikuandmete kaitsele.

32 Võttes arvesse eeltoodut, palub VAS selgitada, kas määruse artikleid 24 ja 32 tuleb tõlgendada nii, et ainuüksi õigusvastase tagajärje teke, mis seisnes isikuandmete loata avalikustamises või neile loata juurdepääsus määruse artikli 4 punkti 12 tähenduses, tõendab seda, et vastutava töötleja võetud tehnilised ja korralduslikud meetmed ei olnud asjakohased.

Teine küsimus (juhul, kui vastus esimesele küsimusele on eitav)

33 Kuna tehniliste ja korralduslike meetmete valik ja rakendamine on jäetud vastutava töötleja subjektiivse hinnangu hooleks ning kuulub tema kaalutlusõiguse alla, tekib VASil küsimus, milline peab olema õiguspärasuse kohtuliku kontrolli ese ja ulatus hindamaks, kas vastutava töötleja võetud tehnilised ja korralduslikud meetmed on asjakohased ning kooskõlas määruse artiklitega 24 ja 32.

34 VAS kahtleb, kas piisab sellest, kui kohus tuvastab, mil viisil on vastutav töötleja nimetatud sätetest tulenevaid kohustusi täitnud, või peab kohus rakendatud tehnilisi ja korralduslikke meetmeid sisuliselt kontrollima, kuigi neid on määruses ainult näitlikult loetletud ning neid peab rakendama eesmärgipärasusest tulenevalt.

Kolmas küsimus (juhul, kui vastus esimesele küsimusele on eitav)

35 Määruse artikli 5 lõike 2 kohaselt vastutab vastutav töötleja sama artikli lõike 1 põhimõtete, mis käsitlevad isikuandmete töötlemist, täitmise eest ning peab olema võimeline selle sätte täitmist tõendama. Määruse artikli 24 lõige 1 kohustab vastutavat töötlejat „rakenda[ma] asjakohaseid tehnilisi ja korralduslikke meetmeid, et tagada ja suuta tõendada isikuandmete töötlemist kooskõlas käesoleva määrusega“.

36 Määruse artikli 82 lõige 3 võimaldab vastutaval töötlejal või volitatud töötlejal vabaneda vastutusest lõike 2 kohaselt, „kui ta tõendab, et ei ole mingil viisil vastutav kahju põhjustanud sündmuse eest“. Vastavalt mainitud lõikele 2 vastutab vastutav töötleja kahju eest, mis on tekkinud sellise töötlemise tulemusel, millega rikutakse käesolevat määrust.

37 Liikmesriigi õiguse kohaselt on kohtumenetluse iga pool kohustatud tõendama asjaolusid, millest ta oma nõuded või vastuväited tuletab. Analoogsetes menetlustes jaotasid esimese astme kohtud tõendamiskoormise kaebajate ja vastustajate vahel erinevalt.

38 Käesolevas asjas on oluline küsimus, kas vastutuse põhimõtet, mis on sätestatud määruse artikli 5 lõikes 2 koostoimes põhjendusega 74 ja artiklis 24, tuleb tõlgendada nii, et need sätted pööravad tõendamiskoormise ümber ning vastutav töötleja, kelle vastu on määruse rikkumise tõttu kahju hüvitamise nõue esitatud, peab vastustajana tõendama, et tema rakendatud tehnilised ja korralduslikud meetmed on asjakohased.

39 Lisaks küsimusele määrusest tulenevate kohustuste täitmise kohtuliku kohtrolli eseme ja ulatuse kohta, on küsitav ka see, kuidas ning milliste tõendite põhjal tuleb kontrollida, kas kõnealuseid kohustusi täideti ning eelkõige, kas rakendati kõiki asjakohaseid tehnilisi ja korralduslikke meetmeid.

40 Menetluses esitas NAP tõendid teabevõrkude kaitse tagamise kohta vastavalt dokumentides määratletud standarditele, kuid küsimata jäeti tehnilise kohtuekspertiisi eksperdiarvamus, mis oleks võimaldanud tuvastada, kas tehnilised ja korralduslikud meetmed olid määruse tähenduses asjakohased. VAS on teadlik, et niisugune vastutav töötleja nagu NAP on kohustatud rakendama võrgu- ja infoturbe korralduslikke, tehnoloogilisi ja tehnilisi meetmeid, mis on proportsionaalses seoses küberkuritegevusest tulenevate ohtudega, et minimeerida nende realiseerumise riski. Samas võib kohtuekspertiisi ekspertide juurdepääs andmetele tuua mis tahes menetluses, mille alus on määruse artikkel 82, endaga kaasa uusi negatiivseid tagajärgi isikuandmete kaitse suhtes.

41 Võttes arvesse tehnika arengu taset, infovõrkude süsteemide kaitse olemasolevaid standardeid ning aset leidnud lubamatut andmetele juurdepääsu häkkerite rünnaku tagajärjel, mille korraldasid isikud, kes ei kuulu vastutava töötleja administratsiooni, tekib VASil küsimus, kas kohus saab tehnilise kohtuekspertiisi eksperdiarvamuse küsimist pidada vajalikuks ja piisavaks tõendiks, et tuvastada, kas vastutava töötleja võetud ja rakendatud tehnilised ja korralduslikud meetmed olid isikuandmete kaitse tagamiseks asjakohased.

Neljas küsimus

42 NAP vastutab töötlemises osaleva vastutava töötlejana, kuid artikli 82 lõike 3 kohaselt saab ta vastutusest vabaneda, kui ta tõendab, et ei ole mingil viisil vastutav kahju põhjustanud sündmuse eest.

43 Menetluses ei ole vaidlust selle üle, et isikuandmetele juurdepääs tekkis NAPi vastu korraldatud häkkerite rünnaku abil. Samas ei põhjustatud loata juurdepääsu ja isikuandmete avalikustamist mitte isikuandmete töötlemise käigus NAPi töötajate poolt või seoses niisuguse töötlemisega.

44 VAS palub tuvastada, kas käesoleval juhul on võimalik eeldada, et tegemist on asjaoluga, mille eest vastutav töötaja ei ole mingil viisil vastutav ning et see asjaolu vabastab ta vastutusest.

Viies küsimus

45 Andmesubjekt palub hüvitada mittemateriaalse kahju, mis väljendub mures, hirmus, stressis, ebakindluses ning kartuses tema isikuandmete tulevase kuritarvitamise pärast, mille erinevaid võimalusi on ta kirjeldanud. Puuduvad tõendid, et VB isikuandmeid oleks kuritarvitatud.

46 Nagu nähtub määruse põhjendustest 75 ja 85, võetakse materiaalse ja mittemateriaalse kahju näidete loetlemisel arvesse isikuandmete laadi ja andmesubjektile tekkinud negatiivseid tagajärgi, mitte üksnes isiku subjektiivset tunnetust.

47 Määruse põhjenduses 146 määratakse kindlaks vastutuse piirid. Vastutus hõlmab „kahju“, mida füüsilisele isikule võib põhjustada töötlemine, mis ei ole määrusega kooskõlas.

48 Pärast seda, kui andmetele juurdepääs on juba saadud, võivad andmesubjekti isikuandmed muutuda erinevate materiaalsete ja mittemateriaalsete kuritarvituste esemeks, millel on märkimisväärsed tagajärjed. Niisugused kuritarvituste juhtumid on avalikkuses teatavaks saanud ning see võib põhjustada suuremat muret häkkerite rünnaku ohvriks langenud isikute seas. Kuna puuduvad andmed juba toimunud kuritarvitamise kohta, on tulevane kuritarvitamine käesoleval juhul pelgalt oletus, hüpotees, mis kätkeb võimalikku, kuid ebaselget ohtu andmesubjekti õigustele.

49 Eeltoodud põhjustel tekib küsimus, kas andmesubjekti negatiivsed tunded niisuguses kontekstis, st kas üksnes asjaolu, et on tekkinud isikuandmete võimaliku tulevase kuritarvituse oht, kuulub mittemateriaalse kahju laialt tõlgendatava mõiste alla ning kujutab endast kahju hüvitamise alust vastavalt määruse artikli 82 lõikele 1 koostoimes põhjendusega 146.

50 Siiski on võimalik, et määruse artikli 82 lõiget 1 koostoimes põhjendusega 146 ei saa tõlgendada nii, et andmesubjekti mis tahes negatiivne tunne, hirm või mure annab õiguse nõuda mittemateriaalse kahju hüvitamist, kui sellele eelnevalt ei ole toimunud isikuandmete ebaseaduslikku kasutamist, näiteks varast ilmajäämise, andmesubjekti nimel laenulepingute sõlmimise või identiteedivarguse teel.