Zbirka odločb sodne prakse

SKLEPNI PREDLOGI GENERALNEGA PRAVOBRANILCA
GIOVANNIJA PITRUZZELLE,
predstavljeni 27. aprila 2023 [1]

Zadeva C-340/21

VB
proti
Natsionalna agentsia za prihodite

(Predlog za sprejetje predhodne odločbe, ki ga je vložilo Varhoven administrativen sad (vrhovno upravno sodišče, Bolgarija))

„Predhodno odločanje – Varstvo osebnih podatkov – Uredba (EU) 2016/679 – Odgovornost upravljavca – Varnost obdelave – Kršitev varnosti obdelave osebnih podatkov – Nepremoženjska škoda, nastala zaradi neukrepanja upravljavca – Odškodninska tožba“

Ali je lahko nezakonito razširjanje osebnih podatkov, do katerega pride zaradi hekerskega napada na javno agencijo, ki hrani te podatke, podlaga za povrnitev nepremoženjske škode posamezniku, na katerega se ti osebni podatki nanašajo, zgolj zaradi njegovega strahu pred morebitno zlorabo teh podatkov v prihodnje? Kakšna so merila, na podlagi katerih je mogoče odgovornost pripisati upravljavcu? Kako naj bi se v okviru sodnega postopka porazdelilo dokazno breme? Kakšen je obseg sodnega nadzora?

I. Pravni okvir

1. Člen 4 Uredbe 2016/679 [2] (v nadaljevanju: Uredba), naslovljen „Opredelitev pojmov“, določa:

„V tej uredbi:

[…]

12. ‚kršitev varstva osebnih podatkov‘ pomeni kršitev varnosti, ki povzroči nenamerno ali nezakonito uničenje, izgubo, spremembo, nepooblaščeno razkritje ali dostop do osebnih podatkov, ki so poslani, shranjeni ali kako drugače obdelani;

[…]“.

[1] Jezik izvirnika: italijanščina.

[2] Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov).

2. Člen 5, naslovljen „Načela v zvezi z obdelavo osebnih podatkov“, določa:

„1. Osebni podatki so:

[…]

(f) obdelujejo se na način, ki zagotavlja ustrezno varnost osebnih podatkov, vključno z zaščito pred nedovoljeno ali nezakonito obdelavo ter pred nenamerno izgubo, uničenjem ali poškodbo z ustreznimi tehničnimi ali organizacijskimi ukrepi (‚celovitost in zaupnost‘).

2. Upravljavec je odgovoren za skladnost z odstavkom 1 in je to skladnost tudi zmožen dokazati (‚odgovornost‘).“

3. Člen 24 te uredbe, naslovljen „Odgovornost upravljavca“, določa:

„1. Ob upoštevanju narave, obsega, okoliščin in namenov obdelave, pa tudi tveganj za pravice in svoboščine posameznikov, ki se razlikujejo po verjetnosti in resnosti, upravljavec izvede ustrezne tehnične in organizacijske ukrepe, da zagotovi in je zmožen dokazati, da obdelava poteka v skladu s to uredbo. Ti ukrepi se pregledajo in dopolnijo, kjer je to potrebno.

2. Kadar je to sorazmerno glede na dejavnosti obdelave, ukrepi iz odstavka 1 vključujejo izvajanje ustreznih politik za varstvo podatkov s strani upravljavca.

3. Zavezanost k odobrenim kodeksom ravnanja iz člena 40 ali izvajanje odobrenega mehanizma potrjevanja iz člena 42 se lahko uporabi za dokazovanje izpolnjevanja obveznosti upravljavca.“

4. Člen 32, naslovljen „Varnost obdelave“, določa:

„1. Ob upoštevanju najnovejšega tehnološkega razvoja in stroškov izvajanja ter narave, obsega, okoliščin in namenov obdelave, pa tudi tveganj za pravice in svoboščine posameznikov, ki se razlikujejo po verjetnosti in resnosti, upravljavec in obdelovalec z izvajanjem ustreznih tehničnih in organizacijskimi ukrepov zagotovita ustrezno raven varnosti glede na tveganje, vključno med drugim z naslednjimi ukrepi, kot je ustrezno:

[…]

2. Pri določanju ustrezne ravni varnosti se upoštevajo zlasti tveganja, ki jih pomeni obdelava, zlasti zaradi nenamernega ali nezakonitega uničenja, izgube, spremembe, nepooblaščenega razkritja ali dostopa do osebnih podatkov, ki so poslani, shranjeni ali kako drugače obdelani.

3. Zavezanost k odobrenemu kodeksu ravnanja iz člena 40 ali izvajanje odobrenega mehanizma potrjevanja iz člena 42 se lahko uporabi za dokazovanje izpolnjevanja zahtev iz odstavka 1 tega člena.

[…]“.

5. Člen 82 te uredbe, naslovljen „Pravica do odškodnine in odgovornost“, določa:

„1. Vsak posameznik, ki je utrpel premoženjsko ali nepremoženjsko škodo kot posledico kršitve te uredbe, ima pravico, da od upravljavca ali obdelovalca dobi odškodnino za nastalo škodo.

2. Vsak upravljavec, vključen v obdelavo, je odgovoren za škodo, ki jo povzroči obdelava, ki krši to uredbo. […].

3. Upravljavec ali obdelovalec je izvzet od odgovornosti iz odstavka 2, če dokaže, da v nobenem primeru ni odgovoren za dogodek, ki povzroči škodo.“

II. Dejansko stanje, postopek in vprašanja za predhodno odločanje

6. V bolgarskih medijih je bila 15. julija 2019 objavljena novica, da je prišlo do nepooblaščenega dostopa do informacijskega sistema Natsionalna agentsia za prihodite (nacionalna agencija za javne prihodke, Bolgarija; v nadaljevanju: NAP)[3] in da so bili na spletu objavljeni različni podatki v zvezi z davki in socialno varnostjo več milijonov ljudi, med katerimi so bili tako bolgarski državljani kot tujci.

7. Več oseb, med katerimi je tudi VB, vlagateljica kasacijske pritožbe v postopku v glavni stvari, je zato zoper NAP vložilo tožbo za povrnitev nepremoženjske škode.

8. V obravnavani zadevi je vlagateljica kasacijske pritožbe v postopku v glavni stvari pri Administratibven sad Sofia-grad (upravno sodišče v Sofiji, Bolgarija, v nadaljevanju: ASSG), vložila tožbo, s katero je zatrjevala, da je NAP kršila nacionalne predpise in ni izpolnila obveznosti, v skladu s katero bi morala glede na to, da ima vlogo upravljavke, osebne podatke obdelovati tako, da bi z izvajanjem ustreznih tehničnih in organizacijskimi ukrepov „zagotovila ustrezno raven varnosti“ v smislu členov 24 in 32 Uredbe št. 679/2016. Vlagateljica kasacijske pritožbe v postopku v glavni stvari je tudi trdila, da ji je nastala nepremoženjska škoda, ki se kaže v skrbeh in strahovih pred zlorabo njenih osebnih podatkov v prihodnosti.

9. Nasprotna stranka v postopku s kasacijsko pritožbo pa je poudarila, da ji vlagateljica kasacijske pritožbe v postopku v glavni stvari ni predložila nobene zahteve po informacijah v zvezi z natančnimi podatki, ki naj bi bili predmet nepooblaščenega dostopa. Poleg tega naj bi se po novici o vdoru v svoj sistem sestala s strokovnjaki za varstvo pravic in interesov državljanov. NAP je ravno tako menila, da med napadom na informacijski sistem in zatrjevano škodo ni nobene vzročne zveze, saj je vse sisteme za vodenje postopkov in upravljanje informacijske varnosti uvedla v skladu z veljavnimi mednarodnimi standardi, ki urejajo to področje.

10. ASSG, ki je odločalo v postopku na prvi stopnji, je tožbo zavrnilo, ker je menilo, da za razširjanje podatkov ni odgovorna NAP, da dokazno breme glede ustreznosti sprejetih ukrepov nosi vlagateljica kasacijske pritožbe in, nazadnje, da ni mogoče povrniti nobene nepremoženjske škode.

11. Zoper sodbo, izdano v postopku na prvi stopnji, je bila nato vložena pritožba pri Varhoven administrativen sad (vrhovno upravno sodišče, Bolgarija). VB, vlagateljica kasacijske pritožbe v postopku v glavni stvari, je med drugim trdila, da je prvostopenjsko sodišče storilo napako pri porazdelitvi dokaznega bremena v zvezi z opustitvijo sprejetja varnostnih ukrepov. Prav tako je menila, da nepremoženjska škoda ne bi smela biti predmet dokaznega bremena, saj gre za škodo, ki je dejanska, in ne zgolj hipotetična.

[3] NAP deluje kot upravljavec v smislu člena 4, točka 7, Uredbe. NAP je v skladu z nacionalnim pravom strokovni upravni organ, podrejen ministru za finance, ki je pristojen za ugotavljanje, zavarovanje in izterjavo javnih in zakonsko določenih zasebnih terjatev države. Pri tem v okviru izvajanja javnih pooblastil, ki so bila prenesena nanjo, obdeluje osebne podatke.

12. NAP pa je ponovno poudarila, da je kot upravljavka sprejela potrebne tehnične in organizacijske ukrepe, in izpodbijala obstoj dokazov o nastanku dejanske nepremoženjske škode. Tesnoba in strahovi naj bi namreč odražali čustveno stanje, za katero naj ne bi bilo mogoče plačati odškodnine.

13. Predložitveno sodišče je ugotovilo, da so se posamezni postopki za povrnitev nepremoženjske škode, ki so jih zoper NAP ločeno začeli oškodovanci, končali z različnimi izidi.

14. V tej okoliščinah je predložitveno sodišče prekinilo odločanje in Sodišču v predhodno odločanje predložilo ta vprašanja:

„1. Ali je treba člena 24 in 32 Uredbe (EU) 2016/679 [Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov)] razlagati tako, da za stališče, da sprejeti tehnični in organizacijski ukrepi niso ustrezni, zadostuje, da so v smislu člena 4, točka 12, Uredbe (EU) 2016/679 osebne podatke nepooblaščeno razkrile ali do njih dostopale osebe, ki niso uslužbenke uprave upravljavca in niso pod njegovim nadzorom?

2. Če je odgovor na prvo vprašanje nikalen, kakšna bi morala biti predmet in obseg sodnega nadzora zakonitosti pri preverjanju, ali so tehnični in organizacijski ukrepi, ki jih je sprejel upravljavec, na podlagi člena 32 Uredbe (EU) 2016/679 ustrezni?

3. Če je odgovor na prvo vprašanje nikalen, ali je treba načelo odgovornosti na podlagi člena 5(2) in člena 24 v povezavi z uvodno izjavo 74 Uredbe (EU) 2016/679 razlagati tako, da v tožbenem postopku na podlagi člena 82(1) Uredbe (EU) 2016/679 dokazno breme za to, da so sprejeti tehnični in organizacijski ukrepi na podlagi člena 32 Uredbe ustrezni, nosi upravljavec? Ali je mogoče pridobitev izvedenskega mnenja šteti za potreben in zadosten dokaz za ugotovitev, ali so bili tehnični in organizacijski ukrepi, ki jih je sprejel upravljavec, v primeru, kot je obravnavani, ustrezni, če sta nepooblaščen dostop do in nepooblaščeno razkritje osebnih podatkov posledica ‚hekerskega napada‘?

4. Ali je treba člen 82(3) Uredbe (EU) 2016/679 razlagati tako, da gre pri nepooblaščenem razkritju ali dostopu do osebnih podatkov v smislu člena 4, točka 12, Uredbe (EU) 2016/679, do katerega pride, kot v obravnavanem primeru, s ‚hekerskim napadom‘ oseb, ki niso uslužbenke uprave upravljavca in niso pod njegovim nadzorom, za dogodek, za katerega upravljavec nikakor ni odgovoren in zaradi katerega ga je upravičeno izvzeti od odgovornosti?

5. Ali je treba člen 82(1) in (2) v povezavi z uvodnima izjavama 85 in 146 Uredbe (EU) 2016/679 razlagati tako, da v primeru, kot je obravnavani primer, v katerem gre za kršitev varstva osebnih podatkov, ki se kaže v nepooblaščenem dostopu do in širjenju osebnih podatkov s ‚hekerskim napadom‘, že skrbi, bojazni in strahovi pred možno zlorabo osebnih podatkov v prihodnosti, ki jih ima posameznik, na katerega se nanašajo osebni podatki, spadajo k pojmu nepremoženjske škode, ki ga je treba razlagati široko, in so podlaga za odškodnino, če taka zloraba ni bila ugotovljena in/ali posamezniku, na katerega se nanašajo osebni podatki, ni nastala nobena druga škoda?“

III. Pravna analiza

A. Uvodne ugotovitve

15. V obravnavani zadevi se postavljajo zanimava in deloma nova vprašanja v zvezi z razlago različnih določb Uredbe. [4]

16. Vseh pet vprašanj za predhodno odločanje se nanaša na isti vidik, to je na pogoje za povrnitev nepremoženjske škode posamezniku, čigar osebni podatki, ki jih hrani javna agencija, so bili po hekerskem napadu objavljeni na spletu.

17. Zaradi poenostavitve bom predlagal ločene jedrnate odgovore na vsa vprašanja za predhodno odločanje, navedena v predložitveni odločbi, čeprav se zavedam, da v njih prihaja do določenega prekrivanja posameznih pojmov glede na to, da so prva štiri vprašanja namenjena opredelitvi pogojev, ki morajo biti izpolnjeni, da bi bilo mogoče odgovornost za kršitev določb Uredbe pripisati upravljavcu, [5] peto vprašanje pa se nanaša zlasti na pojem nepremoženjske škode v smislu povračila te škode. [6]

18. Opozarjam, da Sodišče trenutno obravnava več zadev, ki se nanašajo na člen 82 Uredbe, in da je generalni pravobranilec v eni od teh zadev že predstavil sklepne predloge, ki jih bom upošteval v okviru te analize. [7]

19. Preden se lotim preučevanja postavljenih vprašanj, pa je po mojem mnenju treba podati nekaj uvodnih ugotovitev v zvezi z načeli in cilji Uredbe, ki bodo koristne pri iskanju odgovorov na posamezna vprašanja za predhodno odločanje.

20. V členu 24 Uredbe je na splošno določena obveznost upravljavca, da izvede ustrezne tehnične in organizacijske ukrepe, s katerimi zagotovi in je zmožen dokazati, da je obdelava osebnih podatkov v skladu z Uredbo, v členu 32 te uredbe pa je ta obveznost natančneje določena z vidika varnosti obdelave. Člena 24 in 32 torej natančneje opredeljujeta pravila, ki so že določena v členu 5(2), iz katerega je razvidno, da „[n]ačela v zvezi z obdelavo osebnih podatkov“ vsebujejo tudi „načelo odgovornosti“. To načelo logično izhaja iz „načela celovitosti in zaupnosti“ iz člena 5(1)(f) Uredbe in ga dopolnjuje, pri čemer pa je treba navedeni določbi razlagati ob upoštevanju pristopa, ki temelji na tveganju, na katerem je osnovana Uredba.

[4] To je člena 5(2) (ki določa načelo odgovornosti vseh upravljavcev osebnih podatkov), člena 24 (ki ureja ukrepe, ki jih mora upravljavec izvesti, da zagotovi, da obdelava poteka v skladu s to uredbo), člena 32 (ki navedeno obveznost določa posebej v zvezi z varnostjo obdelave) in člena 82, od (1) do (3) (ki določa pravico do odškodnine za škodo, nastalo zaradi kršitve te uredbe, in možnost, da upravljavec sprejme ukrepe za zagotovitev skladnosti s to uredbo), ter uvodnih izjav 74, 85 in 146, ki so povezane z navedenimi členi Uredbe.

[5] (a) Prvo vprašanje je namenjeno ugotavljanju, ali je mogoče zgolj na podlagi napada na informacijske sisteme sklepati, da vzpostavljeni ukrepi niso ustrezni; (b) drugo vprašanje se nanaša na obseg sodnega nadzora nad ustreznostjo navedenih ukrepov; (c) tretje vprašanje se nanaša na dokazno breme glede same ustreznosti ukrepov in na nekatera tehnična pravila za pridobivanje dokazov; (d) četrto vprašanje pa je upoštevno zaradi ugotavljanja morebitnega izvzetja od odgovornosti, ki je posledica dejstva, da je bil napad na sistem izveden od zunaj.

[6] V zvezi z navedenimi določbami Uredbe je treba navesti, da se prva tri vprašanja nanašajo na vidike odgovornosti upravljavca, povezane z ustreznostjo ukrepov, ki jih je treba sprejeti (členi 5, 24 in 32), četrto in peto vprašanje pa se nanašata na pogoje za izvzetje od odgovornosti in na pojem nepremoženjske škode, ki jo je mogoče povrniti (člen 82).

[7] Glej sklepne predloge generalnega pravobranilca M. Camposa Sánchez-Bordone v zadevi Österreichische Post (Nepremoženjska škoda v zvezi z obdelavo osebnih podatkov) (C-300/21, EU:C:2022:756).

21. Načelo odgovornosti je eden od stebrov, na katerih temelji Uredba, in ena od najpomembnejših novosti, ki se uvajajo s to uredbo. Upravljavcu podatkov namreč nalaga odgovornost za sprejetje ukrepov, s katerimi si dejavno prizadeva za zagotavljanje skladnosti z Uredbo, in za to, da lahko to skladnost tudi dokaže. [8]

22. V pravni teoriji se je razpravljalo o resnični in dejanski kulturni spremembi, ki je posledica „globalnega obsega zahteve po prevzemu odgovornosti“. [9] Pri tem naj ne bi šlo zgolj za formalno izpolnjevanje zakonske obveznosti ali enkraten ukrep, ampak za celovito strategijo, ki jo sprejmejo podjetja in na podlagi katere je mogoče upravljavca, ki zagotavlja skladnost s predpisi na področju varstvu podatkov, izvzeti od odgovornosti.

23. Tehnični in organizacijski ukrepi, ki jih zahteva načelo odgovornosti, morajo biti „ustrezni“, pri njihovem izvajanju pa je treba upoštevati dejavnike, navedene v členu 24 Uredbe, in sicer naravo, obseg, okoliščine in namene obdelave, pa tudi tveganja za pravice in svoboščine posameznikov, ki se razlikujejo po verjetnosti in resnosti.

24. Zato se v skladu s členom 24 Uredbe zahteva, da so izvedeni ukrepi ustrezni, da bi bilo tako mogoče dokazati, da je obdelava v skladu z načeli in določbami te uredbe.

25. S členom 32 Uredbe pa se načelo odgovornosti prenaša na konkretne ukrepe, ki jih je treba sprejeti, da bi se zagotovila „ustrezna raven varnosti glede na tveganje“. V okviru teh prizadevanj so dejavniki, ki so že določeni in ki jih je treba upoštevati pri vzpostavitvi tehničnih in organizacijskih ukrepov, dopolnjeni tudi z najnovejšim tehnološkim razvojem in stroški izvajanja.

26. Pojem ustreznosti zahteva, da rešitve, ki se sprejmejo zaradi zaščite informacijskih sistemov, dosegajo raven sprejemljivosti, tako v tehničnem smislu (upoštevnost ukrepov) kot tudi v smislu kakovosti (učinkovitost zaščite). Posamezna dejanja obdelave morajo biti zaradi zagotavljanja spoštovanja načel nujnosti, ustreznosti in sorazmernosti ne le primerna, ampak tudi zadostna za doseganje ciljev, ki naj bi se z njimi uresničevali. To je torej logika, v kateri ima odločilno vlogo načelo najmanjšega obsega podatkov, v skladu s katerim si je treba v vseh fazah obdelave podatkov stalno prizadevati za čim večje zmanjšanje varnostnih tveganj. [10]

27. Celotna uredba se osredotoča na preprečevanje tveganja in na odgovornost upravljavca ter posledično na teleološki pristop, ki je namenjen doseganju najboljšega možnega rezultata z vidika učinkovitosti, kar pomeni, da je precej odmaknjen od formalistične logike, v skladu s katero je treba za izvzetje od odgovornosti zgolj izpolniti obveznost v zvezi z izvedbo posebnih postopkov. [11]

[8] C. Docksey, *Article 24. Responsibility of the controller*, v C. Kuner, L. A. Bygrave, C. Docksey, L. Drechsler, *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford University Press, 2020, str. 561. Načela in obveznosti, ki izhajajo iz predpisov na področju varstva podatkov, bi morali prežemati kulturo delovanja organizacij na vseh ravneh, ne bi pa se smeli obravnavati kot nabor pravnih zahtev, ki jih mora služba za pravne zadeve zgolj označiti kot izpolnjene.

[9] E. Belisario, G. Riccio, G. Scorza, GDPR e Normativa Privacy - Commentario, Wolters Kluwer, 2022, str. 301.

[10] E. Belisario, G. Riccio, G. Scorza, GDPR, *op.cit*., str. 380.

[11] Zato je jasno, kot bom prikazal v nadaljevanju, da je mogoče na prvo in četrto vprašanje za predhodno odločanje odgovoriti le nikalno. Iz določb Uredbe namreč ni mogoče razbrati nikakršne samodejnosti: zgolj dejstvo, da je prišlo do razkritja osebnih podatkov, ne zadostuje za ugotovitev, da sprejeti tehnični in organizacijski ukrepi niso ustrezni, obenem pa okoliščina, da je do razkritja podatkov prišlo zaradi ukrepanja oseb, ki niso del organizacijske strukture upravljavca in niso pod njegovim nadzorom, ne zadostuje za izvzetje tega upravljavca od odgovornosti.

28. Člen 24 Uredbe ne vsebuje izčrpnega seznama „ustreznih“ ukrepov: zato je treba te ukrepe oceniti v vsakem primeru posebej. To je v skladu s filozofijo Uredbe, iz katere je razvidno, da je treba dati prednost postopkom, ki se sprejmejo na podlagi skrbne ocene konkretnega položaja in na način, ki omogoča čim večjo učinkovitost. [12]

B. Prvo vprašanje za predhodno odločanje

29. Predložitveno sodišče s prvim vprašanjem v bistvu sprašuje, ali je treba člena 24 in 32 Uredbe razlagati tako, da „kršitev varstva osebnih podatkov“, kakor je opredeljena v členu 4, točka 12, Uredbe, sama po sebi zadostuje za ugotovitev, da tehnični in organizacijski ukrepi, ki jih je izvedel upravljavec, niso bili „ustrezni“ za zagotavljanje varstva podatkov.

30. Iz členov 24 in 32 Uredbe izhaja, da mora upravljavec pri izbiri tehničnih in organizacijskih ukrepov, ki jih mora izvesti zaradi zagotavljanja skladnosti z Uredbo, upoštevati vrsto dejavnikov, ki so navedeni v teh členih in našteti v eni od prejšnjih točk teh sklepnih predlogov.

31. Upravljavec ima pri določitvi najustreznejših ukrepov, pri čemer mora upoštevati konkretne okoliščine svojega položaja, sicer nekaj manevrskega prostora, vendar je izbira teh ukrepov v vsakem primeru lahko predmet sodnega nadzora nad skladnostjo izvedenih ukrepov z vsemi obveznostmi in cilji, ki izhajajo iz Uredbe kot take.

32. Natančneje, v zvezi z varnostnimi ukrepi je upravljavec v skladu s členom 32(1) Uredbe zavezan k upoštevanju „najnovejšega tehnološkega razvoja“. To pomeni, da je tehnološka raven ukrepov, ki jih je treba izvesti, omejena na tisto, kar je v trenutku, v katerem so ukrepi sprejeti, razumno mogoče: primernost ukrepa za preprečevanje tveganja mora biti torej v sorazmerju z rešitvami, ki jih trenutno zagotavljajo najnovejša dognanja na področju znanosti, tehnike, tehnologije in raziskav, pri čemer pa je treba, kot bom prikazal v nadaljevanju, upoštevati tudi stroške izvajanja teh ukrepov.

33. Taki ukrepi lahko v določenem trenutku veljajo za „ustrezne“, kljub temu pa se jim lahko storilci kaznivih dejanj v kibernetskem prostoru, ki uporabljajo zelo napredna orodja, s katerimi je mogoče zaobiti tudi varnostne ukrepe, ki sledijo najnovejšemu tehnološkemu razvoju, vseeno izognejo.

34. Po drugi strani pa se kljub skrbnosti, s katero mora obdelovalec vzpostaviti varnostne ukrepe, ne zdi logično, da je nameraval zakonodajalec Unije upravljavcu naložiti obveznost preprečiti kakršno koli kršitev varstva osebnih podatkov. [13]

35. Kot sem že navedel, je Uredba del pristopa, ki ne predvideva nobene samodejnosti in ki zahteva visoko stopnjo odgovornosti upravljavca, kar pa ne sme privesti do položaja, v katerem ta ne bi mogel dokazati, da je ustrezno izpolnil vse svoje obveznosti.

[12] L. Bolognini, E. Pelino, *Codice della disciplina privacy*, Giuffrè, 2019, str. 201. Zakonodajalec Unije se je torej odločil za pristop, ki presega pojmovanje varnosti obdelave, ki temelji na prisotnosti vnaprej določenih varnostnih ukrepov, in sprejel lastno metodologijo za izvajanje mednarodnih standardov na področju upravljanja informacijskih sistemov, ki temelji na tveganju: ta predvideva opredelitev ukrepov za zmanjšanje tveganja, ki niso odvisni od vnaprej pripravljenih in splošno uporabljenih kontrolnih seznamov. Zato se je treba opreti na mednarodne smernice in standarde. Rezultat take ocene tveganja postane zavezujoč, ko organizacija sprejema odločitve za zmanjšanje ugotovljenih tveganj in tako prevzame odgovornost.

[13] Iz pojmovanja ustreznosti ukrepov namreč nedvomno izhaja, da zakonodajalec ni nameraval enakega pomena pripisati vsem tehničnim in organizacijskim ukrepom, ki jih je v abstraktnem smislu mogoče sprejeti. Glej v tem smislu M. Gambini, *Responsabilità e risarcimento nel trattamento dei dati personali*, v. Cuffaro, R. D'Orazio, V. Ricciuto, *I dati personali nel diritto europeo*, Giappichelli, 2019, str. 1059.

36. Poleg tega je v členu 32(1) določeno, da je treba zagotoviti tudi upoštevanje „stroškov izvajanja“ zadevnih tehničnih in organizacijskih ukrepov. Iz tega sledi, da mora ocena ustreznosti takih ukrepov temeljiti na tehtanju med interesi posameznika, na katerega se nanašajo osebni podatki, ki se praviloma nagibajo k zagotavljanju višje ravni varstva, ter gospodarskimi interesi in tehnološko zmogljivostjo upravljavca, ki se po drugi strani nagibajo k zagotavljanju nižje ravni varstva. Pri takem tehtanju je treba upoštevati zahteve splošnega načela sorazmernosti.

37. K navedenim preudarkom je treba z vidika sistematične razlage dodati, da zakonodajalec predvideva možnost, da bo prišlo do napadov na sisteme; v členu 32(1)(c) je namreč med predlaganimi ukrepi navedena tudi zmožnost pravočasne povrnitve razpoložljivosti in dostopa do osebnih podatkov v primeru fizičnega ali tehničnega incidenta. Vključitev take zmožnosti med varnostne ukrepe, s katerimi se zagotavlja ustrezna raven varnosti glede na tveganje, namreč ne bi bila potrebna, če bi se štelo, da napad na sisteme sam po sebi dokazuje, da ti ukrepi niso ustrezni.

C. Drugo vprašanje za predhodno odločanje

38. Predložitveno sodišče z drugim vprašanjem v bistvu sprašuje, kakšna bi morala biti predmet in obseg sodnega nadzora zakonitosti pri preverjanju ustreznosti tehničnih in organizacijskih ukrepov, ki jih je upravljavec osebnih podatkov izvedel v skladu s členom 32 Uredbe.

39. Ker so primeri, do katerih lahko pride v praksi, zelo raznoliki, Uredba, kot je bilo že navedeno, ne predpisuje zavezujočih določb, namenjenih opredelitvi tehničnih in organizacijskih ukrepov, ki jih mora upravljavec sprejeti, da bi izpolnil zahteve te uredbe. Ustreznost sprejetih ukrepov je treba zato presojati v konkretni zadevi, pri tem pa preveriti, ali posebni ukrepi omogočajo razumno preprečevanje tveganja in zmanjšanje negativnih učinkov kršitve.

40. Čeprav nedvomno drži, da se upravljavec o izbiri in izvajanju takih ukrepov odloča na podlagi subjektivne presoje, saj so v Uredbi navedeni zgolj primeri posameznih ukrepov, pa sodnega nadzora ni mogoče omejiti zgolj na preverjanje, ali upravljavec izpolnjuje obveznosti, ki jih ima na podlagi členov 24 in 32, to je na preverjanje, ali je (formalno) predvidel določene tehnične in organizacijske ukrepe. V okviru sodnega nadzora je treba namreč na podlagi dokazov, ki so na voljo sodišču, in okoliščin obravnavane zadeve opraviti konkretno analizo vsebine takih ukrepov, načina, kako se izvajajo, in učinkov, ki jih imajo v praksi. Portugalska vlada je v zvezi s tem prepričljivo ugotovila, da „se zdi, da je način, kako je upravljavec izpolnil svoje obveznosti, neločljivo povezan z vsebino sprejetih ukrepov, s katerimi želi dokazati, da je ob upoštevanju posebne obdelave podatkov (narave, obsega, okoliščin in namenov obdelave), najnovejšega tehnološkega razvoja in razpoložljivih tehnologij ter stroškov, pa tudi tveganj za pravice in svoboščine državljanov, sprejel vse potrebne in ustrezne ukrepe, da bi zagotovil ustrezno raven varnosti glede na tveganje“. [14]

41. Pri sodnem nadzoru je treba zato upoštevati vse dejavnike, navedene v členih 24 in 32 Uredbe, ki, kot sem že navedel, vsebujeta številna merila za ocenjevanje ustreznosti in primere ukrepov, ki jih je mogoče šteti za ustrezne. Poleg tega velja, kot so poudarile Komisija in vse države članice, ki so v zvezi z drugim vprašanjem predložile stališča, da je v členu 32, od (1) do (3), Uredbe izpostavljena potreba po tem, da se zagotovi „ustrezna raven varnosti glede na tveganje“, in da so

[14] Pisno stališče (točka 31).

v njem zato navedeni tudi drugi dejavniki, kot je morebitna uporaba odobrenega kodeksa ravnanja ali odobrenega mehanizma potrjevanja, iz člena 40 oziroma 42 Uredbe, ki ju lahko sprejme upravljavec.

42. Sprejetje kodeksov ravnanja ali mehanizmov potrjevanja je lahko koristen element pri presoji, ki se opravlja v zvezi z izpolnjevanjem obveznosti glede dokaznega bremena in s tem povezanega sodnega nadzora. Vendar je treba pri tem pojasniti, da zgolj zavezanost upravljavca k spoštovanju kodeksa ravnanja ni dovolj, ampak mora upravljavec v skladu z načelom odgovornosti tudi dokazati, da je dejansko sprejel konkretne ukrepe, ki so predvideni v takem kodeksu. Po drugi strani pa je potrdilo „samo po sebi dokaz za to, da dejanja obdelave potekajo v skladu z Uredbo, čeprav ga je mogoče v praksi ovreči“. [15]

43. Nazadnje velja opozoriti, da je treba zadevne ukrepe v skladu s členom 24(1) po potrebi pregledati in dopolniti. Tudi v tem primeru gre za vidik, ki ga bo moralo presoditi nacionalno sodišče. Člen 32(1) Uredbe [16] namreč upravljavcu nalaga obveznost stalnega nadzora in spremljanja pred začetkom izvajanja dejavnosti obdelave in po njej, pa tudi obveznost ohranjanja in morebitnega dopolnjevanja sprejetih ukrepov, da bi se tako preprečile kršitve in po potrebi omejili učinki kršitev.

44. Zato se nagibam k stališču, da sodba, ki bo izdana v tej zadevi, ne bi smela vsebovati seznama bistvenih elementov, kakršnega predlaga portugalska vlada. [17] To bi namreč lahko privedlo do nasprotujočih si razlag, saj je očitno, da tak seznam nikakor ne more biti izčrpen.

D. Tretje vprašanje za predhodno odločanje

45. Predložitveno sodišče s prvim delom tretjega vprašanja Sodišče v bistvu sprašuje, ali je mogoče v okviru odškodninske tožbe, vložene v smislu člena 82 Uredbe, ob upoštevanju načela odgovornosti iz člena 5(2) in člena 24 v povezavi z uvodno izjavo 74 [18] te uredbe šteti, da nosi dokazno breme glede ustreznosti tehničnih in organizacijskih ukrepov iz člena 32 upravljavec osebnih podatkov.

46. Na podlagi ugotovitev, ki sem jih navedel v prejšnjih točkah teh sklepnih predlogov, lahko na to vprašanje na kratko odgovorim pritrdilno.

[15] M. Gambini, *Responsabilità*, *op. cit.*, str. 1067. Posedovanje potrdila pomeni, da se lahko dokazno breme obrne v korist upravljavca, saj lahko tako precej enostavneje dokaže, da je ravnal v skladu z obveznostmi, ki jih ima na podlagi Uredbe.

[16] Navedeni člen v točki (d) izrecno določa, da ocena ustreznosti zajema tudi učinkovitost sprejetih ukrepov, ki jo je treba tako v začetni fazi kot tudi občasno redno testirati, ocenjevati in vrednotiti, da se zagotovi dejanska varnost vseh vrst obdelave ne glede na raven tveganja; v točki (c) pa izrecno določa, da je treba z izvajanjem tehničnih in organizacijskih ukrepov omogočati pravočasno povrnitev razpoložljivosti in dostopa do osebnih podatkov v primeru fizičnega ali tehničnega incidenta. Glej M. Gambini, *Responsabilità*, *op. cit.*, str. 1064 in 1065.

[17] Točka 30 pisnega stališča: „upravljavec bo moral dokazati, da je ocenil vse dejavnike in okoliščine v zvezi z zadevno obdelavo, zlasti pa rezultat opravljene analize tveganja, ugotovljena tveganja, konkretne ukrepe za zmanjšanje teh tveganj, razloge za ukrepe, za katere se je odločil ob upoštevanju tehnoloških rešitev, ki so na voljo na trgu, učinkovitost ukrepov, medsebojno odvisnost tehničnih in organizacijskih ukrepov, usposabljanje osebja, odgovornega za obdelavo podatkov, obstoj zunanjega izvajanja postopkov obdelave podatkov, vključno z razvojem in vzdrževanjem informacijskih tehnologij, ter obstoj nadzora, ki ga opravlja upravljavec, in natančnih navodil, ki jih osebam, pooblaščenim za obdelavo podatkov, zagotovi obdelovalec v smislu člena 28 SUVP; da je ocenil infrastrukturo, s katero zagotavlja podporo informacijskim in komunikacijskim sistemom, ter da je določil raven tveganja za pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki“.

[18] V uvodni izjavi 74 je navedeno: „Uvesti bi bilo treba pristojnost in odgovornost upravljavca glede vsake obdelave osebnih podatkov, ki jo izvede upravljavec ali je izvedena v njegovem imenu. Upravljavec bi moral zlasti izvajati ustrezne in učinkovite ukrepe ter biti zmožen dokazati skladnost dejavnosti obdelave s to direktivo, vključno z učinkovitostjo ukrepov. Ti ukrepi bi morali upoštevati naravo, obseg, okoliščine in namene obdelave ter tveganje za pravice in svoboščine posameznikov.“

47. Glede na besedilo, sobesedilo in cilje Uredbe je namreč mogoče nedvoumno ugotoviti, da dokazno breme nosi upravljavec.

48. Iz besedila več določb Uredbe izhaja, da mora biti upravljavec „zmožen“ ali „sposoben“ „dokazati“, da izpolnjuje obveznosti, ki jih ima na podlagi Uredbe, in zlasti, da je v ta namen izvedel ustrezne ukrepe, kot je navedeno v uvodni izjavi 74, členu 5(2) in členu 24(1). Portugalska vlada poudarja, da je v uvodni izjavi 74 pojasnjeno, da mora dokazno breme, ki ga torej nosi upravljavec, zajemati tudi dokaze v zvezi z „učinkovitostjo [zadevnih] ukrepov“.

49. Zdi se mi, da to dobesedno razlago podpirajo tudi praktični in teleološki preudarki, ki jih predstavljam v nadaljevanju.

50. V zvezi s porazdelitvijo dokaznega bremena je treba ugotoviti, da mora posameznik, na katerega se nanašajo osebni podatki, v okviru odškodninske tožbe, vložene na podlagi člena 82 Uredbe, dokazati, prvič, da je prišlo do kršitve določb te uredbe, drugič, da je utrpel škodo, in tretjič, da med zadevno kršitvijo in škodo obstaja vzročna zveza, kot je bilo navedeno v vseh pisnih stališčih, ki so jih stranke predložile v zvezi s petim vprašanjem za predhodno odločanje. Gre torej za tri kumulativne pogoje, kar je razvidno tudi iz ustaljene sodne prakse Sodišča in Splošnega sodišča na področju nepogodbene odgovornosti Unije.[19]

51. Kljub temu menim, da obveznosti vlagateljice kasacijske pritožbe v postopku v glavni stvari, da dokaže obstoj kršitve Uredbe, ni mogoče razširiti do te mere, da bi morala dokazati, da tehnični in organizacijski ukrepi, ki jih je izvedel upravljavec, v smislu členov 24 in 32 te uredbe niso ustrezni.

52. Kot poudarja Komisija, bi bilo take dokaze v praksi pogosto skoraj nemogoče predložiti, saj posamezniki, na katere se nanašajo osebni podatki, praviloma nimajo niti zadostnega znanja, da bi take ukrepe lahko analizirali, niti dostopa do vseh informacij, ki so na voljo upravljavcu sporne obdelave podatkov, zlasti glede metod, ki so bile uporabljene za zagotavljanje varnosti te obdelave. Poleg tega bi se včasih lahko zgodilo, da upravljavec teh dejstev posameznikom, na katere se nanašajo osebni podatki, ne bi želel razkriti, pri čemer bi trdil, da ima za to utemeljene razloge, in sicer, da ne želi objaviti informacij v zvezi s svojim delovanjem ali celo informacij, za katere velja obveznost varovanja poklicne skrivnosti, na kar bi se lahko med drugim skliceval prav na podlagi varnostnih razlogov.

53. Če bi se torej štelo, da dokazno breme nosi posameznik, na katerega se nanašajo osebni podatki, bi to v praksi pomenilo, da bi se obseg pravice do pravnega sredstva iz člena 82(1) precej zmanjšal. Menim, da to ne bi bilo v skladu z namero zakonodajalca Unije, ki si je s sprejetjem te uredbe prizadeval za okrepitev pravic posameznikov, na katere se nanašajo osebni podatki, in obveznosti obdelovalcev v primerjavi s pravicami in obveznostmi, ki so jih ti imeli na podlagi Direktive 95/46, ki jo je nadomestil s to uredbo. Zato je bolj logično, da mora upravljavec v okviru obrambe, ki jo pripravi kot odziv na odškodninsko tožbo, dokazati, da je s sprejetjem ukrepov, ki so dejansko ustrezni, izpolnil obveznosti iz členov 24 in 32 Uredbe, kar vzdrži tudi pravno presojo.

[19] Glej zlasti sodbi Sodišča z dne 5. septembra 2019, Evropska unija/Guardian Europe in Guardian Europe/Evropska unija (C-447/17 P in C-479/17 P, EU:C:2019:672, točka 147), in z dne 28. oktobra 2021, Vialto Consulting/Komisija (C-650/19 P, EU:C:2021:879, točka 138), ter sodbi Splošnega sodišča z dne 13. januarja 2021, Helbert/EUIPO (T-548/18, EU:T:2021:4, točka 116), in z dne 29. septembra 2021, Kočner/Europol (T-528/20, neobjavljena, EU:T:2021:631, točka 61), kjer je bilo opozorjeno, da morajo biti izpolnjeni tri pogoji, in sicer „mora biti ravnanje, ki se očita instituciji Unije, nezakonito, škoda dejanska, med ravnanjem institucije in zatrjevano škodo pa mora obstajati vzročna zveza“.

54. Predložitveno sodišče z drugim delom tretjega vprašanja Sodišče v bistvu sprašuje, ali je mogoče šteti, da je mnenje sodnega izvedenca potreben in zadosten dokaz za presojo ustreznosti tehničnih in organizacijskih ukrepov, ki jih izvaja upravljavec osebnih podatkov, v primeru, v katerem sta nepooblaščen dostop do osebnih podatkov in razkritje teh podatkov posledica hekerskega napada.

55. Kot so (v bistvu) poudarile bolgarska in italijanska vlada, Irska in Komisija, tudi sam menim, da mora odgovor na postavljena vprašanja temeljiti na ustaljeni sodni praksi, v skladu s katero velja, da je treba, če na posameznem področju ne obstajajo predpisi Unije, postopkovna pravila, ki urejajo sodne postopke, namenjene varstvu pravic posameznikov, na podlagi načela procesne avtonomije določiti v notranjem pravnem redu vsake države članice, vendar le če ta pravila v položajih, ki jih ureja pravo Unije, niso manj ugodna od tistih, ki urejajo podobne položaje v nacionalnem pravu (načelo enakovrednosti), in če ta pravila v praksi ne onemogočajo ali pretirano otežujejo uresničevanja pravic, ki jih priznava pravo Unije (načelo učinkovitosti).

56. V obravnavani zadevi ugotavljam, da Uredba ne vsebuje nobene določbe, ki bi bila namenjena opredelitvi dopustnih načinov predložitve dokazov in njihove dokazne vrednosti, zlasti v zvezi s preiskovalnimi ukrepi (kot je izvedensko poročilo), ki jih nacionalna sodišča lahko ali morajo odrediti, da bi presodila, ali je upravljavec osebnih podatkov sprejel ustrezne ukrepe v smislu Uredbe. Zato menim, da je treba glede na to, da na tem področju ni harmoniziranih predpisov, taka postopkovna pravila določiti v notranjem pravnem redu vsake države članice, pri čemer pa je treba spoštovati načeli enakovrednosti in učinkovitosti.

57. To „načelo učinkovitosti“, ki pomeni, da mora nepristransko presojo opraviti neodvisno sodišče, pa bi bilo lahko ogroženo, če bi se pridevnik „zadosten“ razlagal v smislu, za katerega se zdi, da mu ga pripisuje predložitveno sodišče, in sicer, da je mogoče na podlagi izvedenskega mnenja samodejno sklepati, da so ukrepi, ki jih je sprejel upravljavec, ustrezni. [20]

E. Četrto vprašanje za predhodno odločanje

58. Predložitveno sodišče s četrtim vprašanjem v bistvu sprašuje, ali je treba člen 82(3) Uredbe razlagati tako, da gre v primeru kršitve te uredbe (ki v obravnavani zadevi zajema „nepooblaščeno razkritje“ osebnih podatkov ali „nepooblaščen dostop“ do osebnih podatkov v smislu člena 4, točka 12, Uredbe), ki jo zagrešijo osebe, ki niso uslužbenci upravljavca teh podatkov in niso pod njegovim nadzorom, za dogodek, ki ga nikakor ni mogoče pripisati upravljavcu, in torej za razlog, na podlagi katerega je mogoče upravljavca izvzeti od odgovornosti v smislu člena 82(3).

59. Odgovor na to vprašanje izhaja neposredno iz ugotovitev, ki sem jih navedel v zvezi s samo filozofijo Uredbe: ta namreč ne določa nikakršne samodejnosti, zato upravljavca ni mogoče izvzeti od odgovornosti zgolj na podlagi dejstva, da je do nepooblaščenega razkritja in dostopa do osebnih podatkov prišlo zaradi dejanj ali opustitev oseb, ki niso pod njegovim nadzorom.

60. Najprej je treba na podlagi dobesedne razlage ugotoviti, da niti člen 82(3) niti uvodna izjava 146 Uredbe ne določata nobenih posebnih pogojev, ki jih mora upravljavec izpolniti, da bi bil lahko izvzet od odgovornosti, razen če ne dokaže, da „v nobenem primeru ni odgovoren za dogodek, ki povzroči škodo“. Iz navedenega besedila po eni strani izhaja, da je lahko upravljavec

[20] Pisno stališče (točka 39).

izvzet od odgovornosti le, če dokaže, da ni odgovoren za dogodek, ki je povzročil zadevno škodo, po drugi strani pa je, kot je izpostavila Komisija, iz uporabe izraza „v nobenem primeru“ mogoče razbrati, da je dokazni standard, ki ga zahteva ta določba, visok. [21]

61. Sistem odgovornosti, ki je določen v členu 82 in, splošneje, v celotni Uredbi, je bil predmet obsežnih razprav med pravnimi teoretiki v različnih državah članicah. Ta sistem namreč vsebuje tradicionalne elemente, ki so značilni za nepogodbeno odgovornost, pa tudi elemente, zaradi katerih se glede na strukturo posameznih določb približuje pogodbeni odgovornosti ali celo določeni vrsti objektivne odgovornosti, in sicer zaradi nevarnosti, ki je neločljivo povezana z dejavnostjo obdelave podatkov. Podrobnejša obravnava teh razprav na tem mestu sicer ni primerna, vendar se po mojem mnenju zdi, da v členu 82 Uredbe ni opredeljen sistem objektivne odgovornosti. [22]

62. Škoda, ki nastane zaradi kršitve varstva osebnih podatkov, je lahko posledica krivdne opustitve sprejetja razumnih tehničnih in organizacijskih ukrepov, ki bi morali biti v vsakem primeru ustrezni za preprečitev nastanka te škode, ob upoštevanju tveganj za pravice in svoboščine posameznikov, povezanih z dejavnostjo obdelave. Zaradi teh tveganj je obveznost preprečevanja in izogibanja škodi strožja, kar posledično pomeni, da se razširi tudi obveznost skrbnega ravnanja, ki jo ima upravljavec osebnih podatkov. Zato je mogoče na podlagi povezane razlage obveznosti, s katerimi se upravljavcem osebnih podatkov, nalagajo določena ravnanja, in obveznosti predložitve razbremenilnih dokazov, ki jo mora izpolniti povzročitelj škode, priti do ugotovitve, ki v primeru odgovornosti za nezakonito obdelavo osebnih podatkov, kot jo določa člen 82 Uredbe, govori v prid priznanju povečane odgovornosti za domnevno krivdno ravnanje. [23]

63. Iz tega izhaja, da ima upravljavec možnost predložitve razbremenilnega dokaza (česar mu sistem objektivne odgovornosti ne bi dopuščal). V zvezi s porazdelitvijo dokaznega bremena pa je treba navesti, da člen 82(3) Uredbe določa ureditev, ki je ugodna za oškodovanca, saj v zvezi s krivdo povzročitelja škode predvideva določeno obliko obrnjenega dokaznega bremena, [24] ki je povsem enaka že navedenemu obrnjenemu dokaznemu bremenu, ki velja v zvezi z dokazovanjem ustreznosti sprejetih ukrepov. Zakonodajalec je s tem pokazal, da se zaveda nevarnosti, povezanih s sprejetjem drugačne porazdelitve dokaznega bremena; če bi se namreč dokazno breme za dokazovanje krivde povzročitelja škode preneslo na oškodovanega posameznika, bi to pretirano poseglo v njegov položaj, kar bi v okviru predpisov, ki se nanašajo na uporabo novih tehnologij, dejansko ogrozilo možnosti za uveljavljanje odškodninskega varstva. Za posameznika, na katerega se nanašajo osebni podatki, bi se lahko tak pristop izkazal za posebej težavnega, saj bi moral rekonstruirati kršitev in imeti dostop do postopkov, zaradi katerih je nastala škoda, ter

[21] V skladu z ustaljeno sodno prakso velja, da je treba izjeme od splošnega pravila razlagati ozko, kar pomeni, da je treba tudi morebitno izvzetje od odgovornosti, ki ga določa člen 82(3) Uredbe, razlagati ozko. Glej po analogiji sodbi z dne 15. oktobra 2020, Association française des usagers de banques (C-778/18, EU:C:2020:831, točka 53), in z dne 5. aprila 2022, Commissioner of An Garda Síochána in drugi (C-140/20, EU:C:2022:258, točka 40).

[22] Civilna odgovornost je običajno opredeljena kot objektivna odgovornost, kadar mora subjekt, ki izvaja določeno dejavnost, sprejeti vse ukrepe, ki jih je v abstraktnem smislu mogoče sprejeti, da bi preprečil nastanek škode, ne glede na to, ali je bil z njimi dejansko seznanjen oziroma ali so bili ti ukrepi ekonomsko vzdržni. Če pa mora tak subjekt sprejeti ukrepe, ki jih mora običajno sprejeti gospodarski subjekt v upoštevni gospodarski panogi, da bi zagotavljal varnost in preprečil škodo, ki lahko nastane zaradi opravljanja zadevne dejavnosti, se za pripisovanje odgovornosti za nastalo škodo praviloma uporablja sistem krivdne odgovornosti. M. Gambini, *Responsabilità*, *op. cit.*, str. 1055.

[23] M. Gambini, *Responsabilità*, *op. cit.*, str. 1059. Podobno velja za stališče, v skladu s katerim za dokazovanje dejstva, da je posamezen subjekt sprejel primerne ukrepe, ni dovolj, da ta zatrjuje, da je ravnal z največjo zahtevano skrbnostjo, ampak mora dokazati obstoj zunanje okoliščine, zaradi katere je nastala škoda in za katero sta značilni nepredvidljivost in neizogibnost, ki sta lastni naključnemu dogodku in primerom višje sile, S. Sica, *Sub art. 82*, v: R. D'Orazio, G. Finocchiaro, O. Pollicino, G. Resta, *Codice della privacy e data protection*, Giuffrè, 2021.

[24] „če *dokaže*, da v nobenem primeru ni odgovoren za dogodek, ki povzroči škodo“ (člen 82(3)).

tako dokazati krivdo upravljavca. Po drugi strani pa je upravljavec v boljšem položaju in lahko predloži razbremenilne dokaze, iz katerih je razvidno, da za dogodek, ki je povzročil škodo, nikakor ni odgovoren. [25]

64. Upravljavec bo moral v skladu z že obravnavanim načelom odgovornosti tudi dokazati, da je storil vse, kar je bilo mogoče, za pravočasno povrnitev razpoložljivosti in dostopa do osebnih podatkov.

65. Če se povrnem k vprašanju predložitvenega sodišča, naj najprej navedem, da je treba glede na vse preudarke, ki sem jih doslej predstavil v zvezi z odgovornostjo upravljavca, ugotoviti, da je lahko upravljavec, kot je bilo že navedeno, sicer izvzet od odgovornosti, če dokaže, da je kršitev posledica dogodka, za katerega nikakor ni odgovoren, ni pa mogoče šteti, da enako velja zgolj zato, ker je tak dogodek povzročila oseba, ki ni pod njegovim nadzorom.

66. Če je upravljavec žrtev napada, ki ga izvedejo storilci kaznivih dejanj v kibernetskem prostoru, se sicer lahko šteje, da upravljavec ni odgovoren za dogodek, ki je povzročil škodo, vendar pa ni mogoče izključiti, da je bil vzrok za zadevni napad malomarnost upravljavca podatkov, saj je neobstoj ali neustreznost varnostnih ukrepov za zaščito zadevnih osebnih podatkov, ki bi jih ta moral izvajati, dejansko olajšala izvedbo tega napada. Presojo dejanskega stanja v posameznem primeru pa bo moralo na podlagi dokazov, ki so mu predloženi, opraviti nacionalno sodišče, ki odloča o zadevi.

67. Poleg tega je na podlagi splošnih izkušenj jasno, da so zunanji napadi na sisteme javnih ali zasebnih upravljavcev velike količine osebnih podatkov veliko pogostejši od napadov, ki jih izvedejo uslužbenci teh upravljavcev. Upravljavec mora zato vzpostaviti ustrezne ukrepe, s katerimi se bo zoperstavil zlasti zunanjim napadom.

68. Nazadnje, s teleološkega vidika je treba opozoriti, da se z Uredbo uresničuje cilj zagotavljanja visoke ravni varstva osebnih podatkov. Sodišče je v zvezi s tem že poudarilo, da iz člena 1(2) Uredbe v povezavi z njenimi uvodnimi izjavami 10, 11 in 13 izhaja, da ta uredba institucijam, organom, uradom in agencijam Unije ter pristojnim organom držav članic nalaga, da zagotovijo visoko raven varstva pravic v zvezi z varstvom osebnih podatkov, zagotovljenih s členom 16 PDEU in členom 8 Listine. [26]

69. Če bi Sodišče sprejelo razlago, v skladu s katero bi moral biti upravljavec v primeru, v katerem je do kršitve Uredbe prišlo zaradi dejanja ali opustitve tretje osebe, samodejno izvzet od odgovornosti v smislu člena 82(3) Uredbe, menim, da taka razlaga ne bi bila združljiva s ciljem varstva osebnih podatkov, ki se uresničuje s tem zakonodajnim aktom, ker bi povzročila zmanjšanje obsega pravic posameznikov, na katere se nanašajo osebni podatki, saj bi bila odgovornost omejena na primere, v katerih kršitev zagrešijo osebe, ki podatke obdelujejo pod vodstvom in/ali nadzorom zadevnega upravljavca.

[25] M. Gambini, *Responsabilità*, *op. cit.*, str. 1060.

[26] Glej v tem smislu sodbo z dne 15. junija 2021, Facebook Ireland in drugi (C-645/19, EU:C:2021:483, točki 44 in 45).

F. Peto vprašanje za predhodno odločanje

70. Nacionalno sodišče s petim vprašanjem Sodišču v bistvu predlaga, naj poda razlago pojma „nepremoženjska škoda“ v smislu člena 82 Uredbe. Natančneje, to sodišče sprašuje, ali je treba člen 82(1) in (2) v povezavi z uvodnima izjavama 85 in 146 Uredbe [27] razlagati tako, da lahko v primeru, v katerem se posledice kršitve te uredbe odražajo v nepooblaščenem dostopu do osebnih podatkov in nepooblaščenem razkritju osebnih podatkov, za katera so odgovorni storilci kaznivih dejanj v kibernetskem prostoru, že samo dejstvo, da se posameznik, na katerega se nanašajo osebni podatki, boji morebitne zlorabe svojih osebnih podatkov v prihodnosti, pomeni obstoj (nepremoženjske) škode, ki je podlaga za nastanek pravice do odškodnine.

71. Čeprav jasnega odgovora na postavljeno vprašanje ni mogoče najti niti v členu 82 niti v uvodnih izjavah Uredbe, ki se nanašajo na odškodnino, pa se lahko iz navedenih določb izluščijo nekateri koristni elementi za nadaljnjo analizo: poleg odškodnine za premoženjsko škodo je mogoče uveljavljati tudi nepremoženjsko škodo; kršitev Uredbe ne pomeni samodejne podlage za nastanek škode, ki jo „povzroči“ taka kršitev, oziroma, natančneje, kršitev varstva osebnih podatkov „lahko […] povzroči“ fizično, premoženjsko ali nepremoženjsko škodo posameznikom; pojem škode je treba glede na sodno prakso Sodišča razlagati „široko“ in na način, ki v celoti odraža cilje Uredbe; posamezniki pa morajo za škodo „ki so jo utrpeli“, prejeti „celotno in učinkovito“ odškodnino.

72. Že iz besedila določb Uredbe je razvidno, da je izključena vsakršna možnost uveljavljanja škode, ki naj bi nastala sama po sebi: glavni cilj civilne odgovornosti, ki jo vzpostavlja Uredba, je, da se posamezniku, na katerega se nanašajo osebni podatki, zagotovi zadoščenje, in sicer ravno s „celotno in učinkovito“ odškodnino za škodo, ki jo je utrpel, ter da se tako ponovno vzpostavi ravnovesje v pravnem položaju, ki je bilo zaradi kršitve pravice negativno spremenjeno. [28]

73. Po drugi strani pa je tudi s sistematičnega vidika, tako kot v okviru prava na področju preprečevanja omejevanja konkurence, jasno, da Uredba določa dva stebra varstva: prvi ima lastnosti javnega prava, saj za kršitve določb Uredbe določa sankcije, drugi pa lastnosti zasebnega prava, saj določa prav civilno odgovornost nepogodbene narave, ki jo je mogoče zaradi domnevno krivdnega ravnanja, za katero so značilni elementi, ki sem jih že obravnaval, vključno z možnostjo predložitve razbremenilnih dokazov, opredeliti kot povečano odgovornost. [29]

[27] V uvodni izjavi 85 je navedeno: „Kršitev varstva osebnih podatkov lahko, če se ne obravnava ustrezno in pravočasno, zadevnim posameznikom povzroči fizično, premoženjsko ali nepremoženjsko škodo […]“. V uvodni izjavi 146 je navedeno: „Upravljavec ali obdelovalec bi moral povrniti vso škodo, ki jo oseba lahko utrpi zaradi obdelave, ki krši to uredbo. Upravljavec ali obdelovalec bi moral biti oproščen odgovornosti, če dokaže, da ni v nobenem primeru odgovoren za škodo. Pojem škode bi bilo treba razlagati široko ob upoštevanju sodne prakse Sodišča na način, ki, v celoti odraža cilje te uredbe. To je brez poseganja v kakršne koli odškodninske zahtevke, ki izhajajo iz kršitve drugih pravil prava Unije ali prava države članice. […]. Posamezniki, na katere se nanašajo osebni podatki, bi morali prejeti celotno in učinkovito odškodnino za škodo, ki so jo utrpeli […]“.

[28] Glej zgoraj navedene sklepne predloge generalnega pravobranilca M. Camposa Sánchez-Bordone (točka 29 in opomba 11). Generalni pravobranilec je v teh sklepnih predlogih ob koncu analize, ki jo je opravil z jezikovnega, zgodovinskega, sistematičnega in teleološkega vidika, pri čemer je izključil „kaznovalno“ naravo škode, ki jo je treba povrniti posameznikom, na katere se nanašajo osebni podatki, na podlagi člena 82 (točke od 27 do 55), pravilno poudaril, da državam članicam po eni strani „ni treba (in pravzaprav tudi ne morejo) izbirati med mehanizmi iz poglavja VIII za zagotavljanje varstva podatkov. V primeru kršitve, zaradi katere ne nastane škoda, ima posameznik, na katerega se nanašajo osebni podatki, […] še vedno (vsaj) pravico vložiti pritožbo pri nadzornem organu“, in po drugi strani, da bi „možnost pridobitve odškodnine ne glede na nastanek škode verjetno spodbudila sprožanje civilnih postopkov, v katerih bi se uveljavljali zahtevki, ki morda ne bi bili vedno upravičeni[…], kar bi za dejavnost obdelave podatkov lahko imelo odvračilne učinke“ (točki 54 in 55).

[29] Zanikanje obstoja pravice do odškodnine za šibke in prehodne občutke ali čustva, povezana s kršitvijo pravil o obdelavi podatkov, naj torej še ne bi pomenilo, da je posamezniku, na katerega se nanašajo osebni podatki, popolnoma odvzeto varstvo (glej v tem smislu zgoraj navedene sklepne predloge generalnega pravobranilca M. Camposa Sánchez-Bordone, točka 115).

74. Prožne razlage [30] pojma (nepremoženjska) škoda zato ni mogoče razširiti do te mere, da bi bilo mogoče šteti, da se je zakonodajalec odrekel zahtevi po določitvi prave in dejanske „škode“.

75. Pravo vsebinsko vprašanje, na katero je treba odgovoriti, se glasi, ali je ugotovitev glede obstoja kršitve in vzročne zveze lahko podlaga za nastanek pravice do odškodnine zgolj zaradi skrbi, bojazni in strahov posameznika, na katerega se nanašajo osebni podatki, pred morebitno zlorabo teh podatkov v prihodnosti, če taka zloraba ni bila ugotovljena in/ali posamezniku, na katerega se nanašajo osebni podatki, ni nastala nobena druga škoda.

76. V skladu z ustaljeno sodno prakso Sodišča je treba pojme, ki se uporabljajo v določbi prava Unije, ki v zvezi z opredelitvijo smisla in obsega teh pojmov ne napotuje izrecno na pravo držav članic, običajno razlagati avtonomno in enotno v celotni Uniji, in sicer ne le ob upoštevanju besedila zadevne določbe, ampak tudi okvira, v katerega se umešča, ciljev, ki jih uresničuje akt, katerega del je, in zgodovine nastanka te določbe. [31]

77. Kot je opozoril generalni pravobranilec M. Campos Sánchez-Bordona, [32] Sodišče ni oblikovalo splošne opredelitve „škode“, ki bi se lahko brez razlikovanja uporabljala na katerem koli področju. [33] V zvezi z nepremoženjsko škodo je mogoče na podlagi sodne prakse Sodišča sklepati, da je treba, če je eden od ciljev razlagane določbe varstvo posameznika ali določene kategorije posameznikov, [34] pojem škode pojmovati široko; v skladu s tem merilom se odškodnina za nepremoženjsko škodo prizna tudi, če v razlagani določbi ni omenjena. [35]

78. Čeprav je na podlagi sodne prakse Sodišča mogoče zagovarjati stališče, da v pravu Unije obstaja – pod zgoraj opisanimi pogoji – načelo povračila nepremoženjske škode, pa se strinjam z generalnim pravobranilcem M. Camposom Sánchez-Bordono, da iz tega ni mogoče izpeljati pravila, da je treba povrniti *vsako* nepremoženjsko škodo, ne glede na njeno resnost. [36]

79. V tem okviru je pomembno razlikovanje med nepremoženjsko škodo, ki jo je treba povrniti, in drugimi *neprijetnostmi, do katerih pride zaradi nespoštovanja zakonodaje*, v zvezi s katerimi zaradi njihove neznatnosti ne nastane nujno pravica do odškodnine. [37]

[30] Oziroma „široke“, kot je navedeno v uvodni izjavi 146.

[31] Glej sodbi z dne 15. aprila 2021, The North of England P & I Association (C-786/19, EU:C:2021:276, točka 48), in z dne 10. junija 2021, KRONE – Verlag (C-65/20, EU:C:2021:471, točka 25).

[32] Glej zgoraj navedene sklepne predloge generalnega pravobranilca M. Camposa Sánchez-Bordone (točka 104).

[33] Prav tako ni pojasnilo, katera – samostojna ali ob upoštevanju nacionalne zakonodaje – metoda razlage je primernejša: to je odvisno od predmeta preučitve. Glej sodbe z dne 10. maja 2001, Veedfald (C-203/99, EU:C:2001:258, točka 27), v zvezi z izdelki z napako; z dne 6. maja 2010, Walz (C-63/09, EU:C:2010:251, točka 21), v zvezi z odgovornostjo letalskega prevoznika in z dne 10. junija 2021, Van Ameyde España (C-923/19, EU:C:2021:475, točka 37 in naslednje), o civilni odgovornosti v zvezi z zahtevki, ki izhajajo iz uporabe motornih vozil.

[34] Na primer potrošniki izdelkov ali žrtve prometnih nesreč.

[35] Na področju paketnih potovanj sodba z dne 12. marca 2002, Leitner (C-168/00, EU:C:2002:163); na področju civilne odgovornosti, ki izhaja iz uporabe motornih vozil, sodbe z dne 24. oktobra 2013, Haasová (C-22/12, EU:C:2013:692, točke od 47 do 50); z dne 24. oktobra 2013, Drozdovs (C-277/12, EU:C:2013:685, točka 40), in z dne 23. januarja 2014, Petillo (C-371/12, EU:C:2014:26, točka 35).

[36] Glej zgoraj navedene sklepne predloge generalnega pravobranilca M. Camposa Sánchez-Bordone (točka 105). Sodišče je na primer potrdilo, da pravo Unije ne nasprotuje nacionalni zakonodaji, v skladu s katero se za izračun odškodnine nepremoženjska škoda, povezana s telesnimi poškodbami zaradi nesreče, razlikuje glede na razloge zanjo; glej sodbo z dne 23. januarja 2014, Petillo (C-371/12, EU:C:2014:26), izrek: pravo Unije ne nasprotuje „nacionalni zakonodaji […], ki določa posebno ureditev za odškodnino za nepremoženjsko škodo, nastalo zaradi lažjih telesnih poškodb zaradi prometnih nesreč z motornimi vozili, ki omejuje odškodnino za takšno škodo, glede na to, kar je dopustno v primeru povračila za isto škodo, ki nastane iz drugih razlogov, kot so te nesreče“.

[37] To razlikovanje je v nekaterih nacionalnih pravnih redih razumljeno kot neizogibna posledica življenja v družbi. Nedavno na področju varstva podatkov v Italiji Tribunale di Palermo, sez. I civile, sodba z dne 05/10/2017, št. 5261, ter Cass Civ. Ord. Sez 6, št. 17383/2020. V Nemčiji glej med drugimi sodbe AG Diez, 07.11.2018 – 8 C 130/18; LG Karlsruhe, 02.08.2019 – 8 O 26/19; in AG Frankfurt am Main, 10.07.2020 – 385 C 155/19 (70). V Avstriji: OGH 6 Ob 56/21k.

80. Sodišče to razliko priznava, ko se na težave in nevšečnosti kot na kategorijo, ki je v razmerju do kategorije škode samostojna, sklicuje na področjih, na katerih meni, da jih je treba kompenzirati. [38]

81. Empirično je mogoče ugotoviti, da vsaka kršitev določbe o varstvu osebnih podatkov pri posamezniku, na katerega se ti podatki nanašajo, praviloma povzroči neki negativen odziv. Odškodnina za sam občutek nezadovoljstva, ker nekdo ni spoštoval prava, bi bila zlahka zamenljiva z nadomestilom ob neobstoju škode, za katerega se, kot sem že navedel, zdi, da ga v obravnavani zadevi na podlagi člena 82 Uredbe ni mogoče določiti.

82. Dejstvo, da je v okoliščinah, kakršne so te v postopku v glavni stvari, možnost zlorabe osebnih podatkov le potencialna in se dejansko še ni uresničila, zadostuje za ugotovitev, da bi posameznik, na katerega se nanašajo osebni podatki, zaradi kršitve Uredbe lahko utrpel nepremoženjsko škodo, če dokaže, da mu je strah pred tako zlorabo v konkretnem in točno določenem primeru povzročil škodo, ki se odraža v dejanski in gotovi čustveni prizadetosti. [39]

83. Meja med samo jezo (ki ne pomeni škode, ki jo je treba povrniti) in pravo nepremoženjsko škodo (ki pa jo je treba povrniti) je zagotovo tanka, vendar bi morala nacionalna sodišča, ki morajo to jezo določiti v vsakem primeru posebej, opraviti skrbno presojo vseh elementov, ki jim jih predloži posameznik, na katerega se nanašajo osebni podatki, ki vloži odškodninski zahtevek in ki bo moral natančno, ne pa zgolj na splošno, navesti konkretne elemente, na podlagi katerih bo mogoče ugotoviti, ali se lahko določi „škoda, ki jo je dejansko utrpel“ zaradi kršitve varstva osebnih podatkov, čeprav ta ne dosega vnaprej določenega praga posebne resnosti: pri tem je pomembno, da ne gre zgolj za subjektivno dojemanje, ki je spremenljivo in odvisno tudi od značajskih in osebnostnih lastnosti, ampak za objektivno opredelitev – sicer neznatnega, vendar dokazljivega – nelagodja, ki ga to povzroči v zvezi s telesnim ali duševnim stanjem ali življenjem tega posameznika v družbi; pomembna je narava zadevnih osebnih podatkov in pomen, ki ga imajo v življenju posameznika, na katerega se ti podatki nanašajo, morebiti pa tudi dojemanje tega konkretnega nelagodja, povezanega s kršitvijo varstva osebnih podatkov, v družbi. [40]

[38] Glej sodbo z dne 23. oktobra 2012, Nelson in drugi (C-581/10 in C-629/10, EU:C:2012:657, točka 51), o razlikovanju med „škodo“ v smislu člena 19 Konvencije o poenotenju nekaterih pravil za mednarodni letalski prevoz, ki je bila sprejeta 28. maja 1999 v Montrealu, in „nevšečnostmi“ v smislu Uredbe št. 261/2004, ki jih je treba v skladu s sodbo z dne 19. novembra 2009, Sturgeon in drugi (C-402/07 in C-432/07, EU:C:2009:716), nadomestiti na podlagi člena 7 navedene uredbe. Zakonodajalec je v tem sektorju – tako kot v sektorju prevoza potnikov po morju in celinskih plovnih poteh, ki je urejen z Uredbo št. 1177/2010 – lahko priznal obstoj abstraktne kategorije, saj sta dejavnik, zaradi katerega ta težava nastane, in bistvo te težave enaka za vse prizadete osebe. Menim, da na področju varstva podatkov tako sklepanje ni mogoče.

[39] Po mnenju Irske so ti preudarki v praksi še posebej pomembni v okviru kibernetske kriminalitete, ker bi ugotovitev, v skladu s katero bi bila vsaka oseba, ki bi jo kršitev prizadela – čeprav v najmanjšem možnem obsegu – upravičena do odškodnine za nepremoženjsko škodo, imela pomembne posledice zlasti za upravljavce v javnem sektorju, ki se financirajo z omejenimi javnimi sredstvi in bi morali skrbeti za uveljavljanje kolektivnih interesov, vključno z izboljšanjem varnosti osebnih podatkov (pisno stališče, točka 72).

[40] Glej zgoraj navedene sklepne predloge generalnega pravobranilca M. Camposa Sánchez-Bordone (točka 116).

IV. Predlog

84. Glede na vse navedeno Sodišču predlagam, naj na vprašanja za predhodno odločanje odgovori:

„Člene 5, 24, 32 in 82 Uredbe 2016/679 je treba razlagati tako, da:

obstoj ‚kršitve varstva osebnih podatkov', kakor je opredeljena v členu 4, točka 12, Uredbe, sam po sebi ne zadostuje za ugotovitev, da tehnični in organizacijski ukrepi, ki jih je izvedel upravljavec, niso bili ‚ustrezni' za zagotavljanje varstva zadevnih podatkov;

mora nacionalno sodišče, ki odloča o zadevi, pri preverjanju ustreznosti tehničnih in organizacijskih ukrepov, ki jih je izvedel upravljavec osebnih podatkov, opraviti nadzor, ki zajema konkretno analizo vsebine zadevnih ukrepov, načina, kako se izvajajo, in učinkov, ki jih imajo v praksi;

mora upravljavec osebnih podatkov v okviru odškodninske tožbe, vložene v smislu člena 82 Uredbe, dokazati ustreznost ukrepov, ki jih je izvedel v skladu s členom 32 te uredbe;

je treba dopustne načine predložitve dokazov in dokazno vrednost tako predloženih dokazov, vključno s preiskovalnimi ukrepi, ki jih nacionalna sodišča lahko ali morajo odrediti, da bi presodila, ali je upravljavec osebnih podatkov sprejel ustrezne ukrepe v smislu Uredbe, v skladu z načelom procesne avtonomije določiti v notranjem pravnem redu vsake države članice, pri tem pa spoštovati načeli enakovrednosti in učinkovitosti, kot sta opredeljeni v pravu Unije;

dejstvo, da je kršitev Uredbe, ki je povzročila zadevno škodo, zagrešila tretja oseba, samo po sebi ni razlog, zaradi katerega bi bil upravljavec izvzet od odgovornosti, in da je izvzetje upravljavca od take odgovornosti v skladu s to določbo mogoče le, če ta dokaže, da za kršitev nikakor ni odgovoren;

škoda, ki se kaže kot strah pred morebitno zlorabo osebnih podatkov v prihodnosti, katere obstoj je posameznik, na katerega se nanašajo osebni podatki, dokazal, lahko pomeni obstoj nepremoženjske škode, ki je podlaga za nastanek pravice do odškodnine, če posameznik, na katerega se nanašajo osebni podatki, dokaže, da je individualno utrpel škodo, ki se odraža v dejanski in gotovi čustveni prizadetosti, kar pa mora nacionalno sodišče, ki odloča o zadevi, preveriti v vsakem primeru posebej".