Zbierka súdnych rozhodnutí

NÁVRHY GENERÁLNEHO ADVOKÁTA
GIOVANNI PITRUZZELLA
prednesené 27. apríla 2023 [1]

Vec C-340/21

VB
proti
Nacionalna agencija za prihodite

[návrh na začatie prejudiciálneho konania, ktorý podal Vărchoven administrativen săd (Najvyšší správny súd, Bulharsko)]

„Návrh na začatie prejudiciálneho konania – Ochrana osobných údajov – Nariadenie (EÚ) 2016/679 – Zodpovednosť prevádzkovateľa – Bezpečnosť spracúvania – Porušenie bezpečnosti spracúvania osobných údajov – Nemajetková ujma, ktorá vznikla v dôsledku nečinnosti prevádzkovateľa – Žaloba o náhradu škody“

Môže nezákonné šírenie osobných údajov, ktoré má v držbe verejná agentúra, v dôsledku hackerského útoku, založiť dotknutej osobe nárok na náhradu nemajetkovej ujmy len z dôvodu, že sa táto osoba obáva možného budúceho zneužitia svojich údajov? Aké sú kritériá pre vyvodenie zodpovednosti voči prevádzkovateľovi? Ako sa má v rámci súdneho konania rozdeliť dôkazné bremeno? Aký je rozsah súdneho prieskumu?

I. Právny rámec

1. Článok 4 s názvom „Vymedzenie pojmov“ nariadenia 2016/679 [2] (ďalej len „nariadenie“) stanovuje:

„Na účely tohto nariadenia:

…

(12) ‚porušenie ochrany osobných údajov‘ je porušenie bezpečnosti, ktoré vedie k náhodnému alebo nezákonnému zničeniu, strate, zmene, neoprávnenému poskytnutiu osobných údajov, ktoré sa prenášajú, uchovávajú alebo inak spracúvajú, alebo neoprávnený prístup k nim

…“

[1] Jazyk prednesu: taliančina.

[2] Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracovávaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov).

2. Článok 5 s názvom „Zásady spracúvania osobných údajov“ stanovuje:

„1. Osobné údaje musia byť:

…

f) spracúvané spôsobom, ktorý zaručuje primeranú bezpečnosť osobných údajov, vrátane ochrany pred neoprávneným alebo nezákonným spracúvaním a náhodnou stratou, zničením alebo poškodením, a to prostredníctvom primeraných technických alebo organizačných opatrení (‚integrita a dôvernosť‘).

2. Prevádzkovateľ je zodpovedný za súlad s odsekom 1 a musí vedieť tento súlad preukázať (‚zodpovednosť‘).“

3. Článok 24 toho istého nariadenia s názvom „Zodpovednosť prevádzkovateľa“ stanovuje:

„1. S ohľadom na povahu, rozsah, kontext a účely spracúvania, ako aj na riziká s rôznou pravdepodobnosťou a závažnosťou pre práva a slobody fyzických osôb, prevádzkovateľ prijme vhodné technické a organizačné opatrenia, aby zabezpečil a bol schopný preukázať, že spracúvanie a vykonáva v súlade s týmto nariadením. Uvedené opatrenia sa podľa potreby preskúmajú a aktualizujú.

2. Ak je to primerané vzhľadom na spracovateľské činnosti, opatrenia uvedené v odseku 1 zahŕňajú zavedenie primeraných politík ochrany údajov zo strany prevádzkovateľa.

3. Dodržiavanie schválených kódexov správania uvedených v článku 40 alebo schválených certifikačných mechanizmov uvedených v článku 42 sa môže použiť ako prvok na preukázanie splnenia povinností prevádzkovateľa.“

4. Článok 32 s názvom „Bezpečnosť spracúvania“ stanovuje:

„1. Prevádzkovateľ a sprostredkovateľ prijmú so zreteľom na najnovšie poznatky, náklady na vykonanie opatrení a na povahu, rozsah, kontext a účely spracúvania, ako aj na riziká s rôznou pravdepodobnosťou a závažnosťou pre práva a slobody fyzických osôb, primerané technické a organizačné opatrenia s cieľom zaistiť úroveň bezpečnosti primeranú tomuto riziku, pričom uvedené opatrenia prípadne zahŕňajú aj:

…

2. Pri posudzovaní primeranej úrovne bezpečnosti sa prihliada predovšetkým na riziká, ktoré predstavuje spracúvanie, a to najmä v dôsledku náhodného alebo nezákonného zničenia, straty, zmeny, neoprávneného poskytnutia osobných údajov, ktoré sa prenášajú, uchovávajú alebo inak spracúvajú, alebo neoprávneného prístupu k takýmto údajom.

3. Dodržiavanie schváleného kódexu správania uvedeného v článku 40 alebo schváleného certifikačného mechanizmu uvedeného v článku 42 sa môže použiť ako prvok na preukázanie súladu s požiadavkami uvedenými v odseku 1 tohto článku.

…“

5. Článok 82 toho istého nariadenia s názvom „Právo na náhradu škody a zodpovednosť“ stanovuje:

„1. Každá osoba, ktorá utrpela majetkovú alebo nemajetkovú ujmu v dôsledku porušenia tohto nariadenia, má právo na náhradu utrpenej škody od prevádzkovateľa alebo sprostredkovateľa.

2. Každý prevádzkovateľ, ktorý sa zúčastnil na spracúvaní, je zodpovedný za škodu spôsobenú spracúvaním, ktoré bolo v rozpore s týmto nariadením. ….

3. Prevádzkovateľ alebo sprostredkovateľ je zbavený zodpovednosti podľa odseku 2, ak sa preukáže [ak preukáže – *neoficiálny preklad*], že nenesie žiadnu zodpovednosť za udalosť, ktorá spôsobila škodu.“

II. Skutkový stav, konanie vo veci samej a prejudiciálne otázky

6. Bulharské médiá 15. júla 2019 šírili informácie o tom, že došlo k neoprávnenému prístupu do informačného systému orgánu Nacionalna agencija za prichodite (Národná agentúra pre verejné príjmy, Bulharsko, ďalej len „NAP“ [3]), a že na internete boli uverejnené rôzne informácie z daňovej oblasti a oblasti sociálneho zabezpečenia týkajúce sa miliónov ľudí, tak občanov, ako aj cudzincov.

7. Mnohé osoby, medzi ktorými je aj V.B., žalobkyňa vo veci samej, zažalovali NAP o náhradu nemajetkovej ujmy.

8. V prejednávanej veci žalobkyňa vo veci samej podala na Administrativen săd Sofija-grad (Správny súd Sofia-mesto, ďalej len „ASSG“) žalobu, v ktorej tvrdila, že NAP porušila vnútroštátne predpisy, ako aj svoju povinnosť spracúvať osobné údaje ako prevádzkovateľ takým spôsobom, ktorý „zaručuje primeranú istotu“, a to tým, že prijme primerané technické a organizačné opatrenia v zmysle článkov 24 a 32 nariadenia č. 679/2016. Žalobkyňa ďalej tvrdila, že utrpela nemajetkovú ujmu, ktorá sa prejavila obavami a strachom z budúceho zneužitia jej osobných údajov.

9. Žalovaná naopak zdôraznila, že nedostala od žalobkyne vo veci samej žiadnu žiadosť o tom, ku ktorým konkrétnym osobným údajom bol získaný prístup. Okrem toho v nadväznosti na správu o útoku uskutočnila stretnutia s expertmi na ochranu práv a záujmov občanov. Podľa NAP chýbala tiež príčinná súvislosť medzi kybernetickým útokom a údajne spôsobenou škodou, keďže agentúra zaviedla všetky systémy riadenia procesov a systémy pre informačnú bezpečnosť v súlade s príslušnými medzinárodnými normami.

10. Prvostupňový súd, ASSG, žalobu zamietol, keďže dospel k záveru, že šírenie údajov nemožno pripísať agentúre, že dôkazné bremeno týkajúce sa primeranosti prijatých opatrení znáša žalobkyňa a napokon, že nemožno nahradiť žiadnu nemajetkovú ujmu.

[3] NAP je prevádzkovateľom v zmysle článku 4 bodu 7 nariadenia. Podľa vnútroštátneho práva je to odborný správny orgán podriadený ministrovi financií, príslušný pre zisťovanie, zabezpečovanie a vymáhanie financií, ako aj pre zisťovanie, zabezpečovanie a vymáhanie verejnoprávnych a zákonom stanovených súkromnoprávnych pohľadávok štátu. V rámci výkonu verejnej moci, ktorá jej bola zverená, spracúva osobné údaje.

11. Prvostupňový rozsudok bol napadnutý kasačným opravným prostriedkom na Vărchoven administrativen săd (Najvyšší správny súd, Bulharsko). Žalobkyňa vo veci samej okrem iného zdôraznila, že súd prvého stupňa pochybil pri rozdelení dôkazného bremena týkajúceho sa neprijatia bezpečnostných opatrení. Predmetom dôkazného bremena by nemala byť ani nemajetková ujma, keďže ide o skutočnú, a nie len o potenciálnu nemajetkovú ujmu.

12. NAP zopakovala, že prijala potrebné technické a organizačné opatrenia ako prevádzkovateľ a spochybnila existenciu dôkazu o skutočnej nemajetkovej ujme. Obavy a strach sú totiž emočnými stavmi, ktoré nezakladajú nárok na náhradu.

13. Vnútroštátny súd konštatoval rozličné výsledky jednotlivých konaní, ktoré poškodení samostatne začali proti NAP na účely náhrady nemajetkovej ujmy.

14. Za týchto okolností vnútroštátny súd prerušil konanie a položil Súdnemu dvoru tieto prejudiciálne otázky:

„1. Majú sa články 24 a 32 nariadenia [Európskeho parlamentu a Rady] (EÚ) 2016/679 [z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov)] vykladať v tom zmysle, že na to, aby sa dalo usúdiť, že prijaté technické a organizačné opatrenia nie sú vhodné, postačuje, že došlo k neoprávnenému poskytnutiu osobných údajov, resp. neoprávnenému prístupu k nim v zmysle článku 4 bodu 12 nariadenia (EÚ) 2016/679 osobami, ktoré nie sú úradníkmi administratívy prevádzkovateľa a nepodliehajú jeho kontrole?

2. V prípade zápornej odpovede na prvú otázku: Aký predmet a rozsah by malo mať súdne preskúmanie zákonnosti pri skúmaní, či sú technické a organizačné opatrenia prijaté prevádzkovateľom primerané podľa článku 32 nariadenia (EÚ) 2016/679?

3. V prípade zápornej odpovede na prvú otázku: Má sa zásada zodpovednosti podľa článku 5 ods. 2 a článku 24 v spojení s odôvodnením 74 nariadenia (EÚ) 2016/679 vykladať v tom zmysle, že v konaní o žalobe podľa článku 82 ods. 1 nariadenia (EÚ) 2016/679 prevádzkovateľ nesie dôkazné bremeno s ohľadom na to, že prijaté technické a organizačné opatrenia podľa článku 32 nariadenia sú primerané? Je možné považovať vypracovanie znaleckého posudku za nevyhnutný a dostatočný dôkazný prostriedok na účely zistenia, či v prípade ako je tento, boli technické a organizačné opatrenia prijaté prevádzkovateľom primerané, ak neoprávnený prístup k osobným údajom a neoprávnené poskytnutie osobných údajov je dôsledkom ‚hackerského útoku'?

4. Má sa článok 82 ods. 3 nariadenia (EÚ) 2016/679 vykladať v tom zmysle, že neoprávnené poskytnutie osobných údajov alebo neoprávnený prístup k nim v zmysle článku 4 bodu 12 nariadenia (EÚ) 2016/679 – v tomto prípade prostredníctvom ‚hackerského útoku' spáchaného osobami, ktoré nie sú úradníkmi administratívy prevádzkovateľa a nepodliehajú jeho kontrole – predstavuje udalosť, za ktorú prevádzkovateľ nenesie žiadnu zodpovednosť a ktorá je základom pre zbavenie zodpovednosti?

5. Má sa článok 82 ods. 1 a 2 v spojení s odôvodneniami 85 a 146 nariadenia (EÚ) 2016/679 vykladať v tom zmysle, že v prípade porušenia bezpečnosti osobných údajov, o aký ide vo veci samej, ku ktorému dôjde formou neoprávneného prístupu a šírenia osobných údajov prostredníctvom ‚hackerského útoku', pod pojem nemajetkovej ujmy, ktorý sa má vykladať

extenzívne, spadajú a na náhradu škody oprávňujú iba starosti, obavy a strach dotknutej osoby pred možným budúcim zneužitím osobných údajov, ak také zneužitie nebolo zistené a/alebo dotknutej osobe nevznikla žiadna ďalšia škoda?“

III. Právna analýza

A. Úvodné pripomienky

15. V prejednávanej veci ide o zaujímavé a sčasti nové otázky týkajúce sa výkladu viacerých ustanovení nariadenia. [4]

16. Všetkých päť prejudiciálnych otázok je zameraných na tú istú tému: podmienky náhrady nemajetkovej ujmy spôsobenej osobe, ktorej osobné údaje v držbe verejnej agentúry boli uverejnené na internete v dôsledku hackerského útoku.

17. V záujme zjednodušenia navrhnem samostatné súhrnné odpovede na všetky prejudiciálne otázky uvedené v návrhu na začatie prejudiciálneho konania, hoci som si vedomý určitého pojmového prekrývania, keďže prvé štyri otázky sú zamerané na určenie podmienok pripísateľnosti porušenia ustanovení nariadenia prevádzkovateľovi [5] a piata otázka sa týka presnejšie pojmu nemajetková ujma na účely náhrady škody. [6]

18. Chcel by som upozorniť na to, že v súčasnosti prebieha pred Súdnym dvorom viacero sporov týkajúcich sa článku 82 nariadenia a že v jednej z nich už boli prednesené návrhy generálneho advokáta, ktoré zohľadním v tejto analýze. [7]

19. Pred preskúmaním nastolených otázok považujem za vhodné uviesť niekoľko úvodných poznámok k zásadám a cieľom nariadenia, ktoré budú užitočné pre riešenie jednotlivých otázok.

20. Článok 24 nariadenia vo všeobecnosti stanovuje povinnosť prevádzkovateľa zaviesť primerané technické a organizačné opatrenia, aby zabezpečil, že spracúvanie osobných údajov je v súlade s nariadením, pričom musí byť schopný to preukázať, zatiaľ čo článok 32 konkrétnejšie stanovuje rovnakú povinnosť, pokiaľ ide o bezpečnosť spracúvania. Články 24 a 32 spresňujú to, čo je už stanovené v článku 5 ods. 2, ktorý medzi „zásady uplatniteľné na spracúvanie osobných údajov“ zavádza „zásadu zodpovednosti“. Tá logicky vyplýva zo „zásady integrity a dôvernosti“ stanovenej v článku 5 ods. 1 písm. f) a dopĺňa ju, a obe sa majú vykladať vo svetle prístupu založeného na riziku, na ktorom je nariadenie založené.

[4] Článok 5 ods. 2 (týkajúci sa zásady zodpovednosti každého prevádzkovateľa zodpovedného za spracúvanie osobných údajov), článok 24 (týkajúci sa opatrení, ktoré má prevádzkovateľ prijať na zabezpečenie toho, aby jeho spracúvanie bolo v súlade s týmto nariadením), článok 32 (týkajúci sa tejto povinnosti konkrétne vo vzťahu k bezpečnosti spracúvania) a článok 82 ods. 1 až 3 (týkajúci sa náhrady škody spôsobenej porušením tohto nariadenia a možnosti prevádzkovateľa prijať opatrenia na zabezpečenie súladu s týmto nariadením), ako aj odôvodnenia 74, 85 a 146, ktoré súvisia s uvedenými článkami.

[5] Teda a) prvá otázka sa týka odpovede na to, či zo samotného narušenia systémov možno vyvodiť neprimeranosť zavedených opatrení; b) druhá otázka sa týka rozsahu súdneho preskúmania primeranosti týchto opatrení; c) tretia otázka sa týka dôkazného bremena ohľadom primeranosti a určitých technických spôsobov hľadania dôkazov; d) štvrtá sa týka významu skutočnosti, že útok na systém prišiel zvonka, na účely zbavenia sa zodpovednosti.

[6] Pokiaľ ide o uvedené ustanovenia nariadenia, prvé tri otázky sa týkajú aspektov zodpovednosti prevádzkovateľa vo vzťahu k primeranosti opatrení, ktoré sa majú prijať (články 5, 24 a 32); štvrtá a piata otázka sa týkajú podmienok zbavenia sa zodpovednosti a pojmu nemajetková ujma zakladajúca nárok na náhradu (článok 82).

[7] Pozri návrhy, ktoré predniesol generálny advokát Campos Sánchez-Bordona vo veci Österreichische Post (Nemajetková ujma súvisiaca so spracúvaním osobných údajov) (C-300/21, EU:C:2022:756).

21. Zásada zodpovednosti je jedným z pilierov nariadenia a jednou z jeho najvýznamnejších inovácií. Ukladá prevádzkovateľovi povinnosť prijať proaktívne opatrenia na zaistenie súladu s nariadením a byť pripravený na jeho preukázanie. [8]

22. V literatúre sa hovorí o skutočnej kultúrnej zmene ako o účinku „globálneho rozsahu povinnosti niesť zodpovednosť“ [9]. Nejde ani tak o formálne dodržiavanie zákonnej povinnosti alebo konkrétneho opatrenia, ale skôr o celkovú prijatú podnikovú stratégiu, ktorá zbavuje prevádzkovateľa zodpovednosti, pretože *dodržiava* právnu úpravu v oblasti ochrany údajov.

23. Technické a organizačné opatrenia vyžadované na základe zásady zodpovednosti musia byť „primerané“ s prihliadnutím na faktory uvedené v článku 24: povaha, rozsah, kontext a účely spracúvania, ako aj pravdepodobnosť a závažnosť rizík vo vzťahu k právam a slobodám fyzických osôb.

24. Článok 24 preto vyžaduje primeranosť opatrení, aby bolo možné preukázať súlad spracúvania so zásadami a ustanoveniami nariadenia.

25. Naproti tomu článok 32 premieta zásadu zodpovednosti na konkrétne opatrenia, ktoré sa majú prijať na zaistenie „úrovne bezpečnosti primeranej riziku“. Tým dopĺňa k už stanoveným faktorom, ktoré sa majú zohľadniť pri príprave technických a organizačných opatrení, najnovšie poznatky a náklady na vykonanie opatrení.

26. Pojem primeranosť vyžaduje, aby riešenia prijaté na zabezpečenie informačných systémov dosiahli úroveň prijateľnosti, a to tak z technického hľadiska (relevantnosť opatrení), ako aj z kvalitatívneho hľadiska (účinnosť ochrany). Na zabezpečenie dodržiavania zásad nevyhnutnosti, relevantnosti a proporcionality musí byť spracúvanie nielen vhodné, ale aj uspokojivé vzhľadom na sledované ciele. V tejto logike zohráva rozhodujúcu úlohu zásada minimalizácie, podľa ktorej sa musí vo všetkých fázach spracúvania údajov neustále usilovať o minimalizáciu bezpečnostných rizík. [10]

27. Celé nariadenie je zamerané na predchádzanie rizikám a zodpovednosť prevádzkovateľa, a teda na teleologický prístup, ktorého cieľom je dosiahnuť čo najlepší výsledok z hľadiska účinnosti, čo je veľmi ďaleko od formalistickej logiky spojenej s jednoduchou povinnosťou dodržiavať konkrétne postupy na účely zbavenia sa zodpovednosti. [11]

[8] DOCKSEY, C.: Article 24. Responsibility of the controller. In: KUNER, C., BYGRAVE, L. A., DOCKSEY, C., DRECHSLER, L.: *The EU General Data Protection Regulation (GDPR): A Commentary*. Oxford University Press, 2020, s. 561. Zásady a povinnosti vyplývajúce z predpisov o ochrane údajov by mali preniknúť do kultúrnej štruktúry organizácií na všetkých úrovniach a nemali by sa považovať za súbor právnych požiadaviek, ktoré má právne oddelenie zaškrtnúť.

[9] BELISARIO, E., RICCIO, G., SCORZA, G.: *GDPR e Normativa Privacy – Commentario*. Wolters Kluwer, 2022, s. 301.

[10] BELISARIO, E., RICCIO, G., SCORZA, G.: c. d., s. 380.

[11] Z tohto dôvodu, ako bude uvedené, na prvú a štvrtú prejudiciálnu otázku nemožno odpovedať inak ako záporne. Z ustanovení nariadenia nemožno vyvodiť žiadny automatizmus: ani samotná skutočnosť, že došlo k sprístupneniu osobných údajov, nestačí na vyvodenie záveru, že prijaté technické a organizačné opatrenia nie sú primerané, ale ani okolnosť, že k tomuto sprístupneniu došlo z dôvodu zásahu osôb mimo organizácie prevádzkovateľa a mimo sféry jeho kontroly, nestačí na to, aby bol prevádzkovateľ zbavený zodpovednosti.

28. Článok 24 neobsahuje taxatívny zoznam „primeraných“ opatrení: bude potrebné vykonať posúdenie od prípadu k prípadu. Je to v súlade s filozofiou nariadenia, z ktorej vyplýva, že sa uprednostnilo, aby sa postupy, ktoré sa majú prijať, vybrali na základe dôkladného posúdenia konkrétnej situácie tak, aby mohli byť čo najúčinnejšie. [12]

B. Prvá prejudiciálna otázka

29. Svojou prvou otázkou sa vnútroštátny súd v podstate pýta, či sa články 24 a 32 nariadenia majú vykladať v tom zmysle, že skutočnosť, že došlo k „porušeniu ochrany osobných údajov“, ako je definované v článku 4 ods. 12, sama osebe postačuje na to, aby sa dospelo k záveru, že technické a organizačné opatrenia vykonané prevádzkovateľom neboli „primerané“ na zabezpečenie ochrany údajov.

30. Zo znenia článkov 24 a 32 nariadenia vyplýva, že prevádzkovateľ musí pri výbere technických a organizačných opatrení, ktoré je povinný zaviesť na zaistenie súladu s týmto nariadením, zohľadniť viaceré hodnotiace faktory uvedené v týchto článkoch a pripomenuté vyššie.

31. Prevádzkovateľ má určitý manévrovací priestor pri určení najvhodnejších opatrení vzhľadom na svoju konkrétnu situáciu, ale uvedená voľba v každom prípade podlieha prípadnému súdnemu preskúmaniu súladu uplatňovaných opatrení so všetkými povinnosťami a cieľmi samotného nariadenia.

32. Najmä v súvislosti s bezpečnostnými opatreniami sa v článku 32 ods. 1 vyžaduje, aby prevádzkovateľ zohľadnil „najnovšie poznatky“. To znamená obmedzenie technologickej úrovne opatrení, ktoré sa majú vykonať na to, čo je rozumne možné v čase prijatia opatrení: vhodnosť opatrenia predchádzať riziku musí zodpovedať riešeniam, ktoré ponúka aktuálny stav vedy, techniky, technológie a výskumu, a ako bude uvedené, aj pokiaľ ide o náklady na vykonanie.

33. Opatrenia môžu byť v danom čase „primerané“ a napriek tomu ich môžu kybernetickí zločinci obchádzať pomocou veľmi sofistikovaných nástrojov, ktoré dokážu prelomiť aj najmodernejšie bezpečnostné opatrenia.

34. Napriek tomu sa zdá nelogické predpokladať, že zámerom normotvorcu Únie bolo uložiť prevádzkovateľovi povinnosť zabrániť akémukoľvek porušeniu ochrany osobných údajov bez ohľadu na starostlivosť pri zavádzaní bezpečnostných opatrení. [13]

35. Ako už bolo uvedené vyššie, nariadenie sa odkláňa od automatizmu a vyžaduje vysokú mieru zodpovednosti prevádzkovateľa, ktorá však nemôže viesť k nemožnosti prevádzkovateľa preukázať, že si riadne splnil povinnosti, ktoré mu boli uložené.

[12] BOLOGNINI, L., PELINO, E.: *Codice della disciplina privacy*. Giuffrè, 2019, s. 201. Normotvorca Únie tak prekračuje koncepciu bezpečnosti spracúvania založenú na existencii vopred stanovených bezpečnostných opatrení a prijíma metodiku vlastnú medzinárodným normám o riadení informačných systémov založených na *riziku*: stanovujú sa opatrenia na zmiernenie rizík, ktoré sú nezávislé od predom nastavených a všeobecne uplatniteľných *kontrolných zoznamov*. Preto je potrebné uchýliť sa k medzinárodným usmerneniam a normám. Výsledok takéhoto posúdenia rizík sa potom stáva záväzným, keď organizácia prijíma rozhodnutia s cieľom zmierniť identifikované riziká, čím sa stáva *zodpovednou*.

[13] Pojem primeranosť jednoznačne poukazuje na zámer nepriznať význam všetkým abstraktne možným technickým a organizačným opatreniam. V tomto zmysle pozri GAMBINI, M.: Responsabilità e risarcimento nel trattamento dei dati personali. In: CUFFARO, V., D'ORAZIO, R., RICCIUTO, V.: *I dati personali nel diritto europeo*. Giappichelli, 2019, s. 1059.

36. Okrem toho článok 32 ods. 1 stanovuje, ako som už uviedol, zohľadnenie „nákladov na vykonanie“ posudzovaných technických a organizačných opatrení. Z toho vyplýva, že posúdenie primeranosti takýchto opatrení musí byť založené na rovnováhe medzi záujmami dotknutej osoby, ktoré vo všeobecnosti smerujú k vyššej úrovni ochrany, a ekonomickými záujmami a technologickou kapacitou prevádzkovateľa, ktoré niekedy smerujú k nižšej úrovni ochrany. Toto vyváženie musí spĺňať požiadavky všeobecnej zásady proporcionality.

37. Vzhľadom na systematický výklad k tomu treba dodať, že normotvorca počíta s možnosťou narušenia systémov; článok 32 ods. 1 písm. c) zahŕňa medzi navrhované opatrenia schopnosť včas obnoviť dostupnosť osobných údajov a prístup k nim v prípade fyzického alebo technického incidentu. Zavedenie bezpečnostných opatrení, ktoré zaisťujú úroveň bezpečnosti zodpovedajúcu riziku takejto schopnosti, by bolo zbytočné, ak by sa vychádzalo z toho, že samotné narušenie systémov predstavuje samo osebe dôkaz o neprimeranosti týchto opatrení.

C. Druhá prejudiciálna otázka

38. Svojou druhou otázkou sa vnútroštátny súd v podstate pýta, aký má byť predmet a rozsah súdneho preskúmania pri overovaní primeranosti technických a organizačných opatrení vykonaných prevádzkovateľom v zmysle článku 32 nariadenia.

39. Vzhľadom na rôznorodosť situácií, ktoré môžu nastať v praxi, sa v nariadení, ako bolo uvedené, nestanovujú záväzné ustanovenia na určenie technických a organizačných opatrení, ktoré musí prevádzkovateľ prijať na splnenie požiadaviek tohto nariadenia. Primeranosť prijatých opatrení sa preto musí posudzovať *in concreto*, skúmaním, či konkrétne opatrenia boli spôsobilé primerane zabrániť riziku a minimalizovať negatívne účinky porušenia.

40. Hoci je nepochybne pravda, že výber a vykonávanie takýchto opatrení patrí do subjektívneho posúdenia prevádzkovateľa, keďže opatrenia uvedené v nariadení sú len príkladmi, súd sa nemôže pri preskúmavaní obmedziť len na kontrolu, či prevádzkovateľ plní svoje povinnosti vyplývajúce z článkov 24 a 32, teda či (formálne) stanovil určité technické a organizačné opatrenia. Musí vykonať konkrétnu analýzu obsahu týchto opatrení, spôsobu, akým boli uplatnené a ich praktických účinkov na základe dôkazov, ktoré má k dispozícii, a okolností konkrétneho prípadu. Ako správne poznamenala portugalská vláda, „spôsob, akým si splnil svoje povinnosti, sa javí ako neoddeliteľný od obsahu prijatých opatrení, na preukázanie, že prevádzkovateľ pri zohľadnení konkrétneho spracúvania údajov (jeho povahy, rozsahu, kontextu a účelov), najnovších poznatkov o dostupných technológiách a ich nákladov, ako aj rizík vo vzťahu k právam a slobodám občanov prijal všetky potrebné a vhodné opatrenia na zaistenie úrovne bezpečnosti zodpovedajúcej príslušnému riziku“ [14].

41. Pri súdnom preskúmaní sa preto budú musieť zohľadniť všetky faktory uvedené v článkoch 24 a 32, ktoré, ako už bolo uvedené, uvádzajú zoznam kritérií na posúdenie primeranosti a uvádzajú príklady opatrení, ktoré možno považovať za primerané. Okrem toho, ako zdôraznila Komisia a všetky členské štáty, ktoré predložili pripomienky k druhej otázke, v článku 32 ods. 1 až 3 sa zdôrazňuje potreba „zaistiť úroveň bezpečnosti primeranú tomuto riziku“, pričom sa na tento účel uvádzajú ďalšie relevantné faktory, ako napríklad prípadné prijatie schváleného kódexu správania alebo schváleného systému certifikácie prevádzkovateľom, ako sa uvádza v článkoch 40 a 42 nariadenia.

[14] Písomné pripomienky, bod 31.

42. Prijatie kódexov správania alebo systémov certifikácie môže ponúknuť užitočný hodnotiaci prvok na účely unesenia dôkazného bremena a súvisiaceho súdneho prieskumu. No so spresnením, že nestačí, aby prevádzkovateľ dodržiaval kódex správania, ale je povinný preukázať, že opatrenia, ktoré tento kódex stanovuje, skutočne prijal v súlade so zásadou zodpovednosti. Naproti tomu, certifikácia predstavuje „sama osebe dôkaz o súlade vykonávaného spracúvania s nariadením, aj keď ho možno v praxi vyvrátiť“ [15].

43. Nakoniec je potrebné uviesť, že tieto opatrenia sa majú podľa článku 24 ods. 1 v prípade potreby prehodnotiť a aktualizovať. A aj to bude predmetom posúdenia vnútroštátneho súdu. Článok 32 ods. 1 nariadenia [16] totiž ukladá prevádzkovateľovi povinnosť neustálej kontroly a monitorovania, pred spracúvaním, ako aj po spracúvaní, ale aj udržiavania a prípadnej aktualizácie prijatých opatrení s cieľom predchádzať porušeniam a prípadne obmedziť ich účinky.

44. Napriek tomu sa prikláňam k vylúčeniu možnosti, aby nadchádzajúci rozsudok obsahoval zoznam podstatných prvkov, ako to navrhuje portugalská vláda [17]. To by mohlo viesť k protichodným výkladom, keďže zoznam samozrejme nikdy nemôže byť vyčerpávajúci.

D. Tretia prejudiciálna otázka

45. Prvou časťou svojej tretej otázky vnútroštátny súd v podstate žiada Súdny dvor, aby určil, či vzhľadom na zásadu zodpovednosti stanovenú v článku 5 ods. 2 a článku 24 v spojení s odôvodnením 74 [18] nariadenia v rámci žaloby o náhradu škody podľa článku 82, znáša dôkazné bremeno týkajúce sa primeranosti technických a organizačných opatrení v zmysle článku 32 prevádzkovateľ zodpovedný za spracúvanie osobných údajov.

46. Predchádzajúce úvahy mi umožňujú stručne odpovedať na túto otázku kladne.

47. Zo znenia zákona, kontextu a cieľov nariadenia totiž jednoznačne vyplýva, že dôkazné bremeno nesie prevádzkovateľ.

48. Zo znenia viacerých ustanovení nariadenia vyplýva, že prevádzkovateľ musí „vedieť“ alebo byť „schopný“ „preukázať“ splnenie svojich povinností vyplývajúcich z nariadenia, a najmä, že na tento účel zaviedol primerané opatrenia, ako sa uvádza v odôvodnení 74, článku 5 ods. 2 a článku 24

[15] GAMBINI, M.: c. d., s. 1067. Držba osvedčenia tak vedie k preneseniu dôkazného bremena v prospech jeho držiteľa, ktorý má uľahčené dokazovanie, že konal v súlade s povinnosťami vyplývajúcimi z nariadenia.

[16] V písmene d) sa výslovne stanovuje, že posúdenie primeranosti sa vzťahuje na účinnosť prijatých opatrení, ktorá sa musí pravidelne testovať, overovať a vyhodnocovať, a to v počiatočnej fáze aj v pravidelných intervaloch, aby sa zabezpečila účinná bezpečnosť všetkých druhov spracúvania bez ohľadu na úroveň ich rizika; a v odseku c) sa ďalej výslovne stanovuje, že zavedené technické a organizačné opatrenia musia mať schopnosť včas obnoviť dostupnosť a prístup osobných údajov v prípade fyzického alebo technického incidentu. Pozri GAMBINI, M.: c. d., s. 1064 – 1065.

[17] Bod 30 písomných pripomienok: „Je úlohou prevádzkovateľa, aby preukázal, ako posúdil všetky faktory a okolnosti súvisiace s predmetným spracúvaním, najmä výsledok vykonanej analýzy rizík, zistené riziká, konkrétne opatrenia nájdené na zmiernenie týchto rizík, odôvodnenie zvolených možností vzhľadom na technologické riešenia dostupné na trhu, účinnosť opatrení, vzájomný vzťah medzi technickými a organizačnými opatreniami, školenie zamestnancov spracúvajúcich údaje, existenciu externého zabezpečovania spracúvania údajov vrátane vývoja a údržby informačných technológií a existenciu dohľadu zo strany prevádzkovateľa a presných pokynov pre spracovateľa podľa článku 28 GDPR v súvislosti so spracúvaním osobných údajov spracovateľmi; ako bola posúdená infraštruktúra podporujúca komunikačné a informačné systémy a ako bola klasifikovaná úroveň rizika vo vzťahu k právam a slobodám dotknutých osôb.“

[18] Podľa odôvodnenia 74: „Mali by sa stanoviť povinnosti a zodpovednosť prevádzkovateľa v súvislosti s akýmkoľvek spracúvaním osobných údajov, ktoré vykonáva sám alebo ktoré sa vykonáva v jeho mene. Prevádzkovateľ by mal byť najmä povinný prijať primerané a účinné opatrenia a vedieť preukázať súlad spracovateľských činností s týmto nariadením vrátane účinnosti opatrení. V uvedených opatreniach by sa mala zohľadniť povaha, rozsah, kontext a účely spracúvania a riziko pre práva a slobody fyzických osôb.“

ods. 1 Ako pripomína portugalská vláda, vyššie uvedené odôvodnenie 74 spresňuje, že dôkazné bremeno takto uložené prevádzkovateľovi, musí zahŕňať dôkaz o „účinnosti predmetných opatrení“.

49. Tento doslovný výklad sa mi zdá byť podporený nasledujúcimi praktickými a teleologickými úvahami.

50. Pokiaľ ide o rozdelenie dôkazného bremena, v rámci žaloby o náhradu škody založenej na článku 82 musí dotknutá osoba, ktorá podala žalobu proti prevádzkovateľovi, preukázať po prvé, že došlo k porušeniu nariadenia, po druhé, že utrpela škodu a po tretie, že existuje príčinná súvislosť medzi predchádzajúcimi dvoma prvkami, ako bolo uvedené vo všetkých písomných vyjadreniach k piatej prejudiciálnej otázke. Tieto tri podmienky sú kumulatívne, ako to vyplýva aj z ustálenej judikatúry Súdneho dvora a Všeobecného súdu v kontexte mimozmluvnej zodpovednosti Únie.[19]

51. Domnievam sa však, že povinnosť žalobkyne preukázať existenciu porušenia nariadenia nemôže ísť tak ďaleko, aby musela preukázať, že technické a organizačné opatrenia vykonané prevádzkovateľom sú neprimerané v zmysle článkov 24 a 32.

52. Ako uvádza Komisia, predloženie takýchto dôkazov by bolo v praxi často takmer nemožné, keďže dotknuté osoby spravidla nemajú dostatočné znalosti na to, aby mohli analyzovať takéto opatrenia, ani prístup ku všetkým informáciám, ktoré má prevádzkovateľ sporného spracúvania k dispozícii, najmä pokiaľ ide o metódy použité na zaistenie bezpečnosti tohto spracúvania. Okrem toho prevádzkovateľ by mohol niekedy tvrdiť, že jeho odmietnutie poskytnúť tieto skutočnosti dotknutým osobám je založené na legitímnom dôvode nezverejňovať svoje vnútorné záležitosti alebo dokonca informácie, na ktoré sa vzťahuje služobné tajomstvo, najmä z bezpečnostných dôvodov.

53. Ak by sa teda dospelo k záveru, že dôkazné bremeno znáša dotknutá osoba, praktickým dôsledkom by bolo, že právo podať žalobu, stanovené v článku 82 ods. 1, by stratilo veľkú časť svojho obsahu. Podľa môjho názoru by to nebolo v súlade so zámermi normotvorcu Európskej únie, ktorý sa prijatím tohto nariadenia snažil posilniť práva dotknutých osôb a povinnosti prevádzkovateľov v porovnaní so smernicou 95/46, ktorú nahradilo. Je preto logickejšie a právne udržateľnejšie, že prevádzkovateľ je povinný v rámci svojej obhajoby k žalobe o náhradu škody preukázať, že splnil svoje povinnosti podľa článkov 24 a 32 uvedeného nariadenia prijatím účinných primeraných opatrení.

54. V druhej časti svojej tretej otázky sa vnútroštátny súd v podstate pýta Súdneho dvora, či možno znalecký posudok považovať za nevyhnutný a dostatočný dôkaz na posúdenie primeranosti technických a organizačných opatrení vykonaných prevádzkovateľom zodpovedným za spracúvanie osobných údajov v situácii, keď k neoprávnenému prístupu k osobným údajom a ich poskytnutiu došlo v dôsledku *hackerského* útoku.

[19] Pozri najmä rozsudky Súdneho dvora z 5. septembra 2019, Európska únia/Guardian Europe a Guardian Europe/Európska únia (C-447/17 P a C-479/17 P, EU:C:2019:672, bod 147), a z 28. októbra 2021,Vialto Consulting/Komisia (C-650/19 P, EU:C:2021:879, bod 138), ako aj rozsudky Všeobecného súdu z 13. januára 2021, Helbert/Eupo (T-548/18, EU:T:2021:4, bod 116), a z 29. septembra 2021, Kočner/Europol (T-528/20, neuverejnený, EU:T:2021:631, bod 61), v ktorých sa pripomína, že musia byť splnené tri podmienky, a to „protiprávnosť konania vytýkaného inštitúcii Únie, existencia skutočnej škody a existencia príčinnej súvislosti medzi konaním tejto inštitúcie a uplatňovanou škodou“.

55. Ako (v podstate) zdôraznili bulharská a talianska vláda, Írsko a Komisia, domnievam sa, že odpoveď na tieto otázky musí vychádzať z našej ustálenej judikatúry, podľa ktorej v súlade so zásadou procesnej autonómie v prípade neexistencie pravidiel Únie v tejto oblasti prináleží vnútroštátnemu právnemu poriadku každého členského štátu stanoviť procesné pravidlá upravujúce súdne konania na ochranu práv jednotlivcov, avšak za predpokladu, že tieto pravidlá nie sú v situáciách upravených právom Únie menej priaznivé ako pravidlá upravujúce podobné situácie upravené vnútroštátnym právom (zásada ekvivalencie) a v praxi neznemožňujú alebo nadmerne nesťažujú výkon práv priznaných právom Únie (zásada efektivity).

56. V tomto prípade konštatujem, že nariadenie neobsahuje žiadne ustanovenie zamerané na určenie prípustných metód dokazovania a ich dôkaznej sily, najmä pokiaľ ide o dôkazné prostriedky (ako je znalecký posudok), ktoré vnútroštátne súdy môžu alebo musia nariadiť na posúdenie toho, či prevádzkovateľ zodpovedný za spracúvanie osobných údajov prijal primerané opatrenia v zmysle nariadenia. Domnievam sa preto, že vzhľadom na neexistenciu harmonizovaných pravidiel v tejto oblasti je na vnútroštátnom právnom poriadku každého členského štátu, aby určil tieto procesné pravidlá za predpokladu dodržania zásad ekvivalencie a efektivity.

57. Vyššie uvedená „zásada efektivity“, z ktorej vyplýva, že nezávislý súd musí vykonať nestranné posúdenie, by mohla byť narušená, ak by sa prídavné meno „dostatočný“ chápalo v tom zmysle, aký mu podľa môjho názoru priznáva vnútroštátny súd a síce, že zo znaleckého posudku možno automaticky vyvodiť, že opatrenia prijaté prevádzkovateľom sú primerané. [20]

E. Štvrtá prejudiciálna otázka

58. Svojou štvrtou otázkou sa vnútroštátny súd v podstate pýta, či sa má článok 82 ods. 3 nariadenia vykladať v tom zmysle, že v prípade porušenia tohto nariadenia (spočívajúceho, ako v prejednávanej veci, v „neoprávnenom poskytnutí“ alebo „neoprávnenom prístupe“ k osobným údajom v zmysle článku 4 ods. 12) osobami, ktoré nie sú zamestnancami prevádzkovateľa zodpovedného za spracúvanie týchto údajov a nie sú pod jeho kontrolou, ide o udalosť, ktorú prevádzkovateľovi v žiadnom prípade nemožno pripísať, a teda je dôvodom zbavenia sa zodpovednosti podľa článku 82 ods. 3.

59. Odpoveď na túto otázku vyplýva lineárne z toho, čo bolo uvedené vyššie o všeobecnej filozofii nariadenia: neexistuje automatizmus, a preto samotná skutočnosť, že k neoprávnenému poskytnutiu osobných údajov alebo prístupu k nim došlo vinou osôb mimo sféry kontroly prevádzkovateľa, nezbavuje prevádzkovateľa zodpovednosti.

60. Po prvé z doslovného hľadiska treba poznamenať, že článok 82 ods. 3, ani odôvodnenie 146 nestanovujú žiadne osobitné podmienky, ktoré prevádzkovateľ môže splniť na to, aby bol zbavený zodpovednosti s výnimkou prípadu, že preukáže, že „nenesie žiadnu zodpovednosť za udalosť, ktorá spôsobila škodu“. Z tohto znenia na jednej strane vyplýva, že prevádzkovateľ sa môže zbaviť zodpovednosti len vtedy, ak preukáže, že za udalosť, ktorá spôsobila predmetnú škodu, nenesie zodpovednosť, a na druhej strane, že miera dokazovania vyžadovaná týmto ustanovením je vzhľadom na použitie výrazu „žiadnu“ vysoká, ako zdôraznila Komisia. [21]

[20] Písomné pripomienky, bod 39.

[21] V súlade s ustálenou judikatúrou Súdneho dvora, podľa ktorej sa výnimky zo všeobecného pravidla majú vykladať reštriktívne, sa každá prípadná výnimka zo zodpovednosti podľa článku 82 ods. 3 má vykladať reštriktívne. Pozri analogicky rozsudky z 15. októbra 2020, Association française des usagers de banques (C-778/18 , EU:C:2020:831, bod 53), a z 5. apríla 2022, Commissioner of An Garda Síochána a i. (C-140/20, EU:C:2022:258, bod 40).

61. Režim zodpovednosti stanovený v článku 82 a všeobecnejšie v celom nariadení bol predmetom rozsiahlej diskusie v literatúre rôznych členských štátov. Obsahuje totiž tradičné prvky typické pre mimozmluvnú zodpovednosť, ale aj prvky, ktoré ho v štruktúre ustanovení približujú k zmluvnej zodpovednosti alebo dokonca k forme objektívnej zodpovednosti vzhľadom na nebezpečnosť, ktorá je vlastná činnostiam spracúvania údajov. Na tomto mieste nie je náležité opisovať celú diskusiu, ale podľa môjho názoru sa zdá, že článok 82 nestanovuje režim objektívnej zodpovednosti. [22]

62. Škoda spôsobená porušením ochrany osobných údajov môže vzniknúť ako zavinený dôsledok neprijatia rozumných a v každom prípade primeraných technických a organizačných opatrení na jej zabránenie s prihliadnutím na riziká vo vzťahu k právam a slobodám osôb spojené s činnosťou spracúvania. Tieto riziká sprísňujú povinnosť predchádzať škode a zabrániť jej, čím sa rozširuje povinnosť náležitej starostlivosti, ktorú má prevádzkovateľ. Zo spoločného výkladu povinností konať, ktoré má prevádzkovateľ, a ustanovenia o oslobodzujúcom dôkaze, ktorý má niesť pôvodca ujmy, možno preto vyvodiť argument v prospech uznania povahy závažnejšej zodpovednosti za predpokladané zavinenie v prípade zodpovednosti za nezákonné spracúvanie osobných údajov, ktorú stanovuje článok 82 nariadenia. [23]

63. Z toho vyplýva možnosť prevádzkovateľa predložiť oslobodzujúci dôkaz (čo nie je povolené pri objektívnej zodpovednosti). Pokiaľ ide o rozloženie dôkazného bremena, článok 82 ods. 3 nariadenia stanovuje priaznivý režim pre poškodeného, pričom stanovuje formu prenesenia dôkazného bremena týkajúceho sa zavinenia pôvodcu ujmy, [24] v úplnej symetrii s vyššie uvedeným prenesením dôkazného bremena, pokiaľ ide o primeranosť prijatých opatrení. Normotvorca tak ukazuje, že si je vedomý nebezpečenstva, ktoré je spojené s prijatím odlišného rozloženia dôkazného bremena; ak by dôkazné bremeno o zavinení pôvodcu ujmy preniesol na poškodeného, v konečnom dôsledku by jeho postavenie preťažil, a tým by vlastne ohrozil funkčnosť ochrany náhrady škody v kontexte pravidiel spojených s využívaním nových technológií. Pre dotknutú osobu by totiž mohlo byť obzvlášť náročné rekonštruovať spôsob vzniku škody a mať k nemu prístup, a v dôsledku toho preukázať zavinenie prevádzkovateľa. Naopak prevádzkovateľ má najlepšiu pozíciu, aby predložil oslobodzujúci dôkaz, ktorým preukáže, že mu nemožno v žiadnom prípade pripísať skutočnosť, ktorá zakladá nárok na náhradu škody. [25]

64. Prevádzkovateľ bude musieť v súlade s vyššie opísanou zásadou zodpovednosti preukázať aj to, že urobil všetko pre to, aby včas obnovil dostupnosť osobných údajov a prístup k nim.

65. Aby som sa vrátil k otázke vnútroštátneho súdu, na základe toho, čo bolo doteraz povedané o povahe zodpovednosti prevádzkovateľa, v prípade, že ako bolo uvedené, sa prevádzkovateľ môže zbaviť zodpovednosti preukázaním, že porušenie bolo spôsobené príčinou, ktorú mu nemožno v nijakom prípade pripísať, samotná skutočnosť, že udalosť bola spôsobená osobou mimo jeho sféry kontroly, nemožno za takú považovať.

[22] Občianskoprávna zodpovednosť sa zvykne kvalifikovať ako objektívna zodpovednosť vždy, keď konajúci subjekt je povinný prijať všetky opatrenia, ktoré sú abstraktne možné na zabránenie vzniku škody, bez ohľadu na to, či o nich skutočne vedel alebo na ich ekonomickú udržateľnosť. Naopak, ak je konajúci subjekt povinný prijať opatrenia, ktoré sú bežne dodržiavané prevádzkovateľom v príslušnom hospodárskom odvetví na účely zachovania bezpečnosti a predchádzania škode, ktorá môže vzniknúť v dôsledku vykonávanej činnosti, pripísanie samotnej škody má tendenciu smerovať k režimu zodpovednosti za konkrétne zavinenie. GAMBINI, M.: c. d., s. 1055.

[23] GAMBINI, M.: c. d. s. 1059. Podobne v prospech názoru, že dôkaz o prijatí primeraných opatrení nespočíva v jednoduchom tvrdení o najvyššej možnej starostlivosti, ale v preukázaní tretej skutočnosti, ktorá viedla ku vzniku škody, majúcej vlastnosti nepredvídateľnosti a nevyhnutnosti, ktoré sú typické pre náhodnú udalosť a vyššiu moc, SICA, S.: Sub art. 82. In: D'ORAZIO, R., FINOCCHIARO, G., POLLICINO, O., RESTA, G.: *Codice della privacy e data protection*. Giuffrè, 2021.

[24] „… ak *preukáže*, že nenesie žiadnu zodpovednosť za udalosť, ktorá spôsobila škodu" (článok 82 ods. 3).

[25] GAMBINI, M.: c. d., s. 1060.

66. Ak sa prevádzkovateľ stane obeťou útoku kybernetických zločincov, udalosť, ktorá viedla ku vzniku škody, by sa mohla považovať za udalosť, ktorú mu nemožno pripísať, ale nie je vylúčené, že na vzniku predmetného útoku sa prevádzkovateľ mohol podieľať svojou nedbanlivosťou, ktorá útok uľahčila v dôsledku neexistencie alebo nedostatočnosti opatrení pre zabezpečenie osobných údajov, ktoré je povinný vykonať. Ide o skutkové posúdenie, ktoré je špecifické pre každý prípad a je ponechané na vnútroštátny súd rozhodujúci o spore, s prihliadnutím na dôkazy, ktoré mu boli predložené.

67. Okrem toho zo všeobecných skúseností vyplýva, že vonkajšie útoky na systémy verejných alebo súkromných subjektov, ktoré majú k dispozícii veľké množstvo osobných údajov, sú oveľa častejšie ako interné útoky. Prevádzkovateľ preto musí zaviesť primerané opatrenia na riešenie najmä vonkajších útokov.

68. Napokon z teleologického hľadiska treba poznamenať, že cieľom nariadenia je dosiahnuť vysokú úroveň ochrany. V tejto súvislosti Súdny dvor už zdôraznil, že z článku 1 ods. 2 nariadenia v spojení s odôvodneniami 10, 11 a 13 tohto nariadenia vyplýva, že toto nariadenie ukladá inštitúciám, orgánom, úradom a agentúram Únie, ako aj príslušným orgánom členských štátov povinnosť zabezpečiť vysokú úroveň ochrany práv zaručených v článku 16 ZFEÚ a článku 8 Charty. [26]

69. Ak by sa Súdny dvor priklonil k výkladu, podľa ktorého by sa prevádzkovateľ automaticky zbavil zodpovednosti podľa článku 82 ods. 3, keď sa porušenia nariadenia dopustila tretia osoba, mal by takýto výklad účinok, ktorý je nezlučiteľný s cieľom ochrany sledovaným týmto nástrojom, pretože by oslabil práva dotknutých osôb, keďže by uvedenú zodpovednosť obmedzil na prípady, keď porušenie spôsobili osoby, ktoré podliehajú právomoci a/alebo kontrole tohto prevádzkovateľa.

F. Piata prejudiciálna otázka

70. Svojou piatou otázkou vnútroštátny súd v podstate žiada Súdny dvor o výklad pojmu „nehmotná ujma“ (v jazyku nariadenia „nemajetková“) v zmysle článku 82 nariadenia. Konkrétne sa pýta, či sa majú ustanovenia článku 82 ods. 1 a 2 nariadenia v spojení s jeho odôvodneniami 85 a 146 [27] vykladať v tom zmysle, že v situácii, keď porušenie tohto nariadenia spočívalo v neoprávnenom prístupe k osobným údajom a neoprávnenom poskytnutí týchto údajov kybernetickými zločincami, môže skutočnosť, že dotknutá osoba sa obáva možného zneužitia svojich osobných údajov v budúcnosti, sama osebe predstavovať (nemajetkovú) ujmu zakladajúcu právo na náhradu.

71. Článok 82 ani odôvodnenia o náhrade škody neposkytujú jasnú odpoveď na túto otázku, avšak možno z nich vyvodiť niektoré užitočné prvky pre analýzu: nehmotná (alebo nemajetková) ujma môže byť predmetom náhrady popri hmotnej (alebo majetkovej) ujme; porušenie nariadenia nevedie automaticky ku škode, ktorá je týmto porušením „spôsobená“, alebo presnejšie,

[26] Pozri v tomto zmysle rozsudok z 15. júna 2021, Facebook Ireland a i. (C-645/19, EU:C:2021:483, body 44 a 45).

[27] Podľa odôvodnenia 85: „Ak sa porušenie ochrany osobných údajov nerieši primeraným spôsobom a včas, môže fyzickým osobám spôsobiť ujmu na zdraví, majetkovú alebo nemajetkovú ujmu.“ Podľa odôvodnenia 146: „Prevádzkovateľ alebo sprostredkovateľ by mali nahradiť akúkoľvek škodu, ktorú môže osoba utrpieť v dôsledku spracúvania, ktoré je v rozpore s týmto nariadením. Prevádzkovateľ alebo sprostredkovateľ by však mali byť tejto zodpovednosti zbavení, ak preukážu, že za škodu nenesú žiadnu zodpovednosť. Podľa judikatúry Súdneho dvora by sa mal pojem škoda vykladať v širokom zmysle spôsobom, ktorý v plnej miere zohľadňuje ciele tohto nariadenia. Týmto nie sú dotknuté prípadné nároky na náhradu škody vyplývajúce z porušenia iných pravidiel stanovených v práve Únie alebo v práve členského štátu… Dotknuté osoby by za utrpenú škodu mali dostať úplnú a účinnú náhradu…“

porušenie ochrany osobných údajov „môže spôsobiť“ fyzickým osobám fyzickú, hmotnú alebo nehmotnú ujmu; pojem škoda by sa mal vykladať „široko“ vzhľadom na judikatúru Súdneho dvora, aby plne odrážal ciele nariadenia; náhrada „utrpenej“ škody by mala byť „úplná a účinná“.

72. Už doslovné znenie ustanovení nariadenia vylučuje akýkoľvek možný náznak škody *in re ipsa*: hlavným cieľom občianskoprávnej zodpovednosti stanovenej v nariadení je poskytnúť dotknutej osobe zadosťučinenie práve prostredníctvom „úplnej a účinnej“ náhrady škody, ktorá jej vznikla a teda obnoviť rovnováhu právneho postavenia, ktoré bolo nepriaznivo zmenené porušením práva. [28]

73. Taktiež aj zo systematického hľadiska, ako je to v práve hospodárskej súťaže, nariadenie stanovuje dva piliere ochrany: jeden verejnoprávnej povahy so stanovením sankcií v prípade porušenia ustanovení nariadenia, jeden súkromnoprávnej povahy so stanovením občianskoprávnej zodpovednosti mimozmluvnej povahy, ktorá môže byť kvalifikovaná ako závažnejšia pre predpokladané zavinenie s vyššie uvedenými charakteristikami, aj s odkazom na oslobodzujúci dôkaz. [29]

74. Extenzívny výklad [30] pojmu (nemajetková) ujma teda nemôže ísť tak ďaleko, aby naznačoval, že normotvorca upustil od potreby existencie skutočnej „škody“.

75. Skutočnou hmotnoprávnou otázkou je, či po preukázaní existencie porušenia a príčinnej súvislosti môže vzniknúť právo na náhradu škody len z dôvodu starostí, obáv a strachu, ktoré pociťuje dotknutá osoba v súvislosti s možným budúcim zneužitím jej osobných údajov, ak sa takéto zneužitie nepreukázalo a/alebo dotknutá osoba neutrpela žiadnu ďalšiu škodu.

76. Podľa ustálenej judikatúry Súdneho dvora pojmy obsiahnuté v ustanovení práva Únie, ktoré na účely určenia svojho zmyslu a pôsobnosti výslovne neodkazuje na právo členských štátov, si v zásade vyžadujú autonómny a jednotný výklad v celej Európskej únii, ktorý treba hľadať s prihliadnutím na doslovné znenie dotknutého ustanovenia, kontext, do ktorého spadá, ciele sledované právnou úpravou, ktorej je súčasťou a na vývoj tohto ustanovenia. [31]

77. Súdny dvor, ako pripomenul generálny advokát Campos Sánchez-Bordona [32], v skutočnosti nesformuloval všeobecnú definíciu „škody“, ktorá by sa bez rozdielu uplatňovala v ktorejkoľvek oblasti. [33] Na účely nemajetkovej ujmy z jeho judikatúry možno vyvodiť, že ak je jedným z cieľov

[28] Pozri už citované návrhy, ktoré predniesol generálny advokát Campos Sánchez-Bordona, bod 29 a poznámka 11. V tých istých návrhoch generálny advokát správne uzavrel svoju analýzu z doslovného, historického, kontextuálneho a teleologického hľadiska tým, že vylúčil „sankčnú“ povahu škody, ktorá sa má dotknutým osobám nahradiť podľa článku 82 (body 27 až 55), pričom na jednej strane konštatuje, že členské štáty „si nemusia (a v skutočnosti ani nemôžu) vybrať spomedzi mechanizmov na zabezpečenie ochrany údajov uvedených v kapitole VIII. V prípade porušenia, ktoré nemá za následok vznik škody, má dotknutá osoba ešte (prinajmenšom) právo podať sťažnosť dozornému orgánu“ a na druhej strane, že „možnosť získať kompenzáciu bez ohľadu na akúkoľvek škodu by pravdepodobne podnecovala občianskoprávne spory, v ktorých by sa uplatňovali nároky, ktoré by možno neboli vždy opodstatnené, a v tomto smere by mohla odradiť od činnosti spočívajúcej v spracúvaní údajov“ (body 54 a 55).

[29] Nepriznanie práva na náhradu škody z dôvodu slabých a dočasných pocitov alebo emócií spojených s porušením predpisov týkajúcich sa spracúvania by teda neznamenalo, že dotknutá osoba zostane bez akejkoľvek ochrany (pozri v tomto zmysle už citované návrhy, ktoré predniesol generálny advokát Campos Sánchez-Bordona, bod 115).

[30] Alebo „v širokom zmysle“, ako je uvedené v odôvodnení 146.

[31] Pozri rozsudky z 15. apríla 2021, The North of England P & I Association (C-786/19, EU:C:2021:276, bod 48), a z 10. júna 2021, KRONE – Verlag (C-65/20, EU:C:2021:471, bod 25).

[32] Pozri už citované návrhy, ktoré predniesol generálny advokát Campos Sánchez-Bordona, bod 104.

[33] Tiež neuviedol, ktorá metóda výkladu – autonómny výklad alebo výklad založený na odkaze na vnútroštátne právne poriadky – sa má uprednostniť: závisí to od skúmanej problematiky. Porovnaj rozsudok z 10. mája 2001, Veedfald (C-203/99, EU:C:2001:258, bod 27), týkajúci sa chybných výrobkov; rozsudok zo 6. mája 2010, Walz (C-63/09, EU:C:2010:251, bod 21), týkajúci sa zodpovednosti leteckých dopravcov, alebo rozsudok z 10. júna 2021, Van Ameyde España (C-923/19, EU:C:2021:475, bod 37 a nasl.), ktorý sa týkal zodpovednosti za škodu spôsobenú prevádzkou motorových vozidiel.

vykladaného ustanovenia ochrana jednotlivca alebo určitej kategórie jednotlivcov,[34] pojem škoda má byť široký; v súlade s uvedeným názorom sa náhrada škody vzťahuje aj na nemajetkovú ujmu, aj keď nie je spomenutá vo vykladanom ustanovení.[35]

78. Hoci judikatúra Súdneho dvora dovoľuje tvrdiť, že v práve Únie existuje za uvedených podmienok zásada náhrady nemajetkovej ujmy, súhlasím s tým, čo povedal generálny advokát Campos, že z nej nemožno vyvodiť pravidlo, podľa ktorého možno nahradiť *každú* nemajetkovú ujmu, a to bez ohľadu na jej závažnosť.[36]

79. V tejto súvislosti je relevantné rozlišovanie medzi nemajetkovou ujmou, ktorú možno *nahradiť*, a inými *nepríjemnosťami odvodenými od nedodržania právnych predpisov*, ktoré vzhľadom na svoj malý význam nevyhnutne nebudú viesť k vzniku práva na náhradu.[37]

80. Súdny dvor uznáva tento rozdiel, keď hovorí o ťažkostiach a nepríjemnostiach ako o kategórii, ktorá je nezávislá od kategórie škody, v oblastiach, v ktorých sa domnieva, že za ne treba poskytnúť náhradu.[38]

81. Empiricky možno konštatovať, že akékoľvek porušenie ustanovenia o ochrane osobných údajov vyvolá nejakú nepriaznivú reakciu dotknutej osoby. Náhrada škody odvodená od samotného pocitu nespokojnosti v prípade, ak iná osoba porušila právny predpis, sa ľahko zamieňa s kompenzáciou bez vzniku škody, ktorá, ako som uviedol, sa nezdá, že je v prejednávanej veci možná podľa článku 82 nariadenia.

82. Skutočnosť, že v prípade okolností, akými sú tie v prejednávanej veci, je zneužitie osobných údajov len potenciálne, a nie skutočné, postačuje na to, aby bolo možné konštatovať, že dotknutá osoba mohla utrpieť nemajetkovú ujmu spôsobenú porušením nariadenia za predpokladu, že dotknutá osoba preukáže, že obava z takéhoto zneužitia jej skutočne a konkrétne spôsobila skutočnú a určitú citovú ujmu.[39]

[34] Napríklad spotrebiteľov výrobkov alebo obetí dopravných nehôd.

[35] V oblasti balíkov cestovných služieb rozsudok z 12. marca 2002, Leitner (C-168/00, EU:C:2002:163), a v oblasti zodpovednosti za škodu spôsobenú prevádzkou motorových vozidiel rozsudky z 24. októbra 2013, Haasová (C-22/12, EU:C:2013:692, body 47 až 50); z 24. októbra 2013, Drozdovs (C-277/12, EU:C:2013:685, bod 40), a z 23. januára 2014, Petillo (C-371/12, EU:C:2014:26, bod 35).

[36] Pozri už citované návrhy, ktoré predniesol generálny advokát Campos Sánchez-Bordona, bod 105. Súdny dvor napríklad uznal, že vnútroštátny predpis, podľa ktorého sa pri výpočte náhrady rozlišuje nemajetková ujma spojená s ujmou na zdraví spôsobenou pri nehode v závislosti od toho, ako k nej došlo, je zlučiteľný s predpismi Únie: pozri rozsudok z 23. januára 2014, Petillo (C-371/12, EU:C:2014:26, výrok): právo Únie nebráni „vnútroštátnej právnej úprave…, ktorá upravuje osobitný režim odškodňovania nemajetkovej ujmy vyplývajúcej z ujmy na zdraví v dôsledku ľahkých zranení spôsobených cestnými dopravnými nehodami, ktorý obmedzuje odškodňovanie takejto ujmy v porovnaní s tým, čo sa uplatňuje v oblasti nápravy rovnakej ujmy z iných dôvodov než v dôsledku týchto nehôd“.

[37] Toto rozlíšenie sa objavuje vo vnútroštátnych právnych poriadkoch ako nevyhnutný dôsledok života v spoločnosti. Pozri nedávne rozhodnutia talianskych súdov týkajúce sa ochrany údajov: Tribunale di Palermo, občianskoprávny senát I, rozsudok 05/10/2017 č. 5261, ako aj Cass. Civ. Ord. Sez. 6, č. 17383/2020. Pokiaľ ide o rozhodnutia nemeckých súdov, pozri najmä AG Diez, 07.11.2018 – 8 C 130/18; LG Karlsruhe, 02.08.2019 – 8 O 26/19, a AG Frankfurt am Main, 10.07.2020 – 385 C 155/19 (70). Pokiaľ ide o rozhodnutia rakúskych súdov, pozri OGH 6 Ob 56/21k.

[38] Pozri rozsudok z 23. októbra 2012, Nelson a i. (C-581/10 a C-629/10, EU:C:2012:657, bod 51), týkajúci sa rozlišovania medzi „škodou“ v zmysle článku 19 Dohovoru o zjednotení niektorých pravidiel pre medzinárodnú leteckú dopravu, uzavretého v Montreale 28. mája 1999, a „nepríjemnosťami“ v zmysle nariadenia č. 261/2004, ktoré možno nahradiť na základe článku 7 tohto nariadenia, podľa rozsudku z 19. novembra 2009, Sturgeon a i. (C-402/07 a C-432/07, EU:C:2009:716). V tejto oblasti – tak ako v oblasti osobnej námornej a vnútrozemskej vodnej dopravy, ktorej sa týka nariadenie č. 1177/2010 – normotvorca bol schopný uznať abstraktnú kategóriu vďaka tomu, že faktor, ktorý vyvoláva ťažkosti, a podstata ťažkostí sú v prípade všetkých dotknutých osôb rovnaké. Domnievam sa, že v oblasti ochrany údajov nemožno dospieť k uvedenému záveru.

[39] Podľa Írska sú tieto úvahy v praxi obzvlášť dôležité v kontexte kybernetickej kriminality, pretože ak by každá osoba, ktorej sa porušenie týka – aj keď len minimálne – mala nárok na náhradu nemajetkovej ujmy, malo by to silný vplyv najmä na prevádzkovateľov vo verejnom sektore, ktorí sú financovaní z obmedzených verejných prostriedkov a mali by skôr slúžiť kolektívnym záujmom vrátane zlepšenia bezpečnosti osobných údajov (písomné pripomienky, bod 72).

83. Hranica medzi samotnými nepríjemnosťami (ktoré nemožno nahradiť) a skutočnou nemajetkovou ujmou (ktorú možno nahradiť) je nejasná, avšak vnútroštátne súdy, ktorým prináleží vymedziť túto hranicu v každom jednotlivom prípade, by mali dôkladne posúdiť všetky prvky, ktoré poskytla dotknutá osoba, ktorá žiada o náhradu škody a ktorá bude mať povinnosť presne, a nie všeobecne, uviesť konkrétne prvky, ktoré môžu viesť k existencii „skutočne utrpenej nemajetkovej ujmy“ z dôvodu porušenia ochrany osobných údajov, aj keď nedosahuje vopred stanovenú hranicu osobitnej závažnosti: dôležité je, že nejde o obyčajné subjektívne vnímanie, ktoré je premenlivé a závislé aj od charakterových a osobnostných prvkov, ale o zobjektívnenie nepohodlia, hoci nepatrného, ale preukázateľného vo vlastnej fyzickej alebo psychickej sfére alebo v rámci vlastných medziľudských vzťahov; povaha dotknutých osobných údajov a ich význam v živote dotknutej osoby a možno aj vnímanie, ktoré v danom okamihu má spoločnosť o tomto konkrétnom nepohodlí spojeného s porušením ochrany údajov. [40]

IV. Návrh

84. Na základe všetkých uvedených skutočností navrhujem, aby Súdny dvor na položené prejudiciálne otázky odpovedal takto:

Články 5, 24, 32 a 82 nariadenia 2016/679 sa majú vykladať v tom zmysle, že:

samotná existencia „porušenia ochrany osobných údajov“, ako je vymedzené v článku 4 bode 12, sama osebe nepostačuje na to, aby sa dospelo k záveru, že technické a organizačné opatrenia vykonané prevádzkovateľom neboli „primerané“ na zaistenie ochrany dotknutých údajov,

pri posudzovaní primeranosti technických a organizačných opatrení vykonaných prevádzkovateľom zodpovedným za spracúvanie osobných údajov musí vnútroštátny súd rozhodujúci o spore vykonať prieskum, ktorý sa rozšíri na konkrétnu analýzu obsahu týchto opatrení, ako aj spôsobu ich vykonania a ich praktických účinkov,

v rámci žaloby o náhradu škody podľa článku 82 tohto nariadenia má prevádzkovateľ zodpovedný za spracúvanie osobných údajov povinnosť preukázať primeranosť opatrení, ktoré vykonal podľa článku 32 tohto nariadenia,

v súlade so zásadou procesnej autonómie prináleží vnútroštátnemu právnemu poriadku každého členského štátu určiť prípustné metódy dokazovania a ich dôkaznú silu vrátane dôkazných prostriedkov, ktoré vnútroštátne súdy môžu alebo musia nariadiť na účely posúdenia, či prevádzkovateľ zodpovedný za spracúvanie osobných údajov vykonal primerané opatrenia v zmysle tohto nariadenia v súlade so zásadami ekvivalencie a účinnosti vymedzenými právom Únie,

skutočnosť, že sa porušenia tohto nariadenia, ktoré spôsobilo predmetnú škodu, dopustila tretia osoba, nie je sama osebe dôvodom na zbavenie zodpovednosti prevádzkovateľa a na to, aby mohol byť zbavený zodpovednosti podľa tohto ustanovenia, musí prevádzkovateľ preukázať, že porušenie mu nemožno v žiadnom prípade pripísať,

[40] Pozri už citované návrhy, ktoré predniesol generálny advokát Campos Sánchez-Bordona, bod 116.

ujma spočívajúca v obave z prípadného budúceho zneužitia osobných údajov, ktorej existenciu dotknutá osoba preukázala, môže predstavovať nemajetkovú ujmu zakladajúcu právo na náhradu škody za predpokladu, že dotknutá osoba preukáže, že osobne utrpela skutočnú a určitú citovú ujmu, čo prináleží overiť v každom jednotlivom prípade vnútroštátnemu súdu rozhodujúcemu o spore.