Zbierka súdnych rozhodnutí

NÁVRHY GENERÁLNEHO ADVOKÁTA
YVES BOT
prednesené 23. septembra 2015 [1]

Vec C-362/14

Maximillian Schrems
proti
Data Protection Commissioner

[návrh na začatie prejudiciálneho konania, ktorý podal High Court (Írsko)]

„Návrh na začatie prejudiciálneho konania — Osobné údaje — Ochrana fyzických osôb pri spracovaní týchto údajov — Charta základných práv Európskej únie — Články 7, 8 a 47 — Smernica 95/46/ES — Článok 25 — Rozhodnutie 2000/520/ES — Prenos osobných údajov do Spojených štátov — Posúdenie primeranosti úrovne ochrany — Sťažnosť fyzickej osoby, ktorej údaje boli prenesené do tretej krajiny — Vnútroštátny dozorný orgán — Právomoci“

I – Úvod

1. Ako Európska komisia konštatovala vo svojom oznámení z 27. novembra 2013 [2], „prenosy osobných údajov sú dôležitým a nevyhnutným prvkom transatlantických vzťahov. Tvoria neoddeliteľnú súčasť obchodných výmen medzi oboma brehmi Atlantiku, a to aj v nových rastúcich digitálnych obchodných odvetviach, ako sú sociálne médiá alebo cloud computing, kde z EÚ do USA prúdia veľké množstvá údajov“ [3].

2. Také obchodné výmeny sú predmetom rozhodnutia Komisie 2000/520/ES z 26. júla 2000 v súlade so smernicou Európskeho parlamentu a Rady 95/46/ES o primeranosti ochrany poskytovanej zásadami „bezpečného prístavu“ a súvisiacimi často kladenými otázkami vydanými Ministerstvom obchodu USA [4]. Toto rozhodnutie tvorí právny základ prenosu osobných údajov z Únie do podnikov so sídlom v Spojených štátoch, ktoré dodržiavajú zásady bezpečného prístavu.

3. Uvedené rozhodnutie v súčasnosti čelí výzve spočívajúcej v umožnení tokov údajov medzi Úniou a Spojenými štátmi a súčasnom zabezpečení vysokej úrovne ochrany týchto údajov, ako to vyžaduje právo Únie.

4. Viaceré nedávne zistenia totiž poukázali na existenciu programov Spojených štátov na zber informácií vo veľkom rozsahu. Tieto zistenia vyvolali vážne obavy, pokiaľ ide o dodržiavanie požiadaviek práva Únie pri prenosoch osobných údajov do podnikov so sídlom v Spojených štátoch a nedostatky režimu bezpečného prístavu.

1 — Jazyk prednesu: francúzština.

2 — Oznámenie Komisie Európskemu parlamentu a Rade s názvom „Obnovenie dôvery v toky údajov medzi EÚ a USA“ [COM(2013) 846 final].

3 — Strana 2.

4 — Ú. v. ES L 215, s. 7; Mim. vyd. 16/001, s. 119.

5. Súdny dvor má na základe prejednávaného návrhu na začatie prejudiciálneho konania spresniť, aký prístup majú vnútroštátne dozorné orgány a Komisia zaujať v prípade, ak zistia nedostatky pri uplatňovaní rozhodnutia 2000/520.

6. Smernica Európskeho parlamentu a Rady 95/46/ES z 24. októbra 1995 o ochrane fyzických osôb pri spracovaní osobných údajov a voľnom pohybe týchto údajov [5] stanovuje v kapitole IV pravidlá týkajúce sa prenosu osobných údajov do tretích krajín.

7. Článok 25 ods. 1 tejto smernice, ktorý je súčasťou uvedenej kapitoly, stanovuje zásadu, že k prenosu osobných údajov, ktoré sa spracovávajú alebo sú určené na spracovanie po prenose, do tretej krajiny môže dôjsť len vtedy, ak príslušná tretia krajina zaistí primeranú úroveň ochrany týchto údajov.

8. Ako normotvorca Únie uvádza v odôvodnení 57 citovanej smernice, prenos osobných údajov do tretej krajiny, ktorá nezaisťuje primeranú úroveň ochrany, sa naopak musí zakázať.

9. Podľa článku 25 ods. 2 smernice 95/46 „adekvátnosť úrovne ochrany, ktorú poskytuje tretia krajina, sa hodnotí vzhľadom na všetky okolnosti týkajúce sa operácie prenosu údajov alebo komplexu operácií prenosu údajov; zvláštna pozornosť sa venuje charakteru údajov, účelu a trvaniu navrhnutej operácie alebo operácií spracovania, krajine pôvodu a krajine konečného určenia, právnym normám aj všeobecným aj sektorovým, platným v príslušnej tretej krajine a profesionálnym predpisom a bezpečnostným opatreniam, ktorým táto krajina vyhovuje“.

10. V súlade s článkom 25 ods. 6 tejto smernice môže Komisia konštatovať, že tretia krajina zaisťuje primeranú úroveň ochrany osobných údajov z dôvodu jej vnútroštátneho práva alebo medzinárodných dohôd. Pokiaľ Komisia prijme rozhodnutie v tomto zmysle, môže dôjsť k prenosu osobných údajov do príslušnej tretej krajiny.

11. Na základe tohto ustanovenia Komisia prijala rozhodnutie 2000/520. Z článku 1 ods. 1 tohto rozhodnutia vyplýva, že „zásady bezpečného prístavu“, vykonávané v súlade s usmernením vyplývajúcim z „často kladených otázok“ [6], sa považujú za také, ktoré zabezpečujú primeranú úroveň ochrany osobných údajov prenášaných z Únie do podnikov so sídlom v Spojených štátoch.

12. Rozhodnutie 2000/520 teda povoľuje prenos osobných údajov z členských štátov do podnikov so sídlom v Spojených štátoch, ktoré sa zaviazali dodržiavať zásady bezpečného prístavu.

13. V prílohe I rozhodnutia 2000/520 sú uvedené viaceré zásady, ktoré podniky môžu dobrovoľne dodržiavať, spolu s limitmi a osobitným systémom kontroly. Počet podnikov, ktoré sa zaviazali dodržiavať tento takzvaný kódex správania, bol v roku 2013 vyšší ako 3 200.

14. Režim bezpečného prístavu spočíva na riešení, ktoré je kombináciou samocertifikácie a samoposúdenia zo strany súkromných podnikov a zásahu verejnej moci.

15. Zásady bezpečného prístavu boli vypracované „na základe porád so zástupcami podnikateľskej sféry a verejnosti s cieľom uľahčenia obchodu medzi Spojenými štátmi a Európskou úniou. Sú určené výlučne na to, aby ich využívali organizácie v USA, ktoré získavajú osobné údaje z Európskej únie a ktoré chcú splniť kritériá bezpečného prístavu a z nich vyplývajúci predpoklad ‚primeranej úrovne‘ ochrany osobných údajov“ [7].

5 — Ú. v. ES L 281, s. 31; Mim. vyd. 13/015, s. 355. Táto smernica bola zmenená a doplnená nariadením Európskeho parlamentu a Rady (ES) č. 1882/2003 z 29. septembra 2003 (Ú. v. EÚ L 284, s. 1; Mim. vyd. 01/004, s. 447) (ďalej len „smernica 95/46“).

6 — Frequently asked questions (ďalej len „FAQ“).

7 — Druhý odsek prílohy I rozhodnutia 2000/520.

16. Zásady bezpečného prístavu, uvedené v prílohe I rozhodnutia 2000/520, stanovujú okrem iného:

— informačnú povinnosť, podľa ktorej „organizácia musí informovať jednotlivcov o dôvodoch, na základe ktorých vo vzťahu k nim zhromažďuje a využíva informácie, o tom, ako sa majú s danou organizáciou skontaktovať v prípade dopytov alebo sťažností, o druhoch tretích strán, ktorým dané informácie poskytuje a o možnostiach a prostriedkoch, ktoré daná organizácia poskytuje jednotlivcom, ak chcú využívanie a poskytovanie takýchto informácií obmedziť. Toto oznámenie musí byť poskytnuté v jasnom a zrozumiteľnom jazyku vtedy, keď sa od jednotlivcov po prvýkrát požaduje poskytnutie osobných informácií danej organizácii alebo čo najskôr po tom ako je to možné, ale v každom prípade pred tým, než daná organizácia využije takéto informácie na účel iný ako ten, na ktorý boli tieto informácie pôvodne zhromaždené alebo spracúvané prenášajúcou organizáciou alebo pred tým, než daná organizácia poskytne tieto informácie po prvýkrát tretej strane“ [8];

— povinnosť organizácií ponúknuť jednotlivcom možnosť rozhodnúť sa, či sa ich osobné informácie môžu poskytnúť tretej strane alebo môžu byť využité na účel, ktorý je nezlučiteľný s cieľom (účelmi), na ktorý (ktoré) boli tieto informácie pôvodne zhromaždené alebo následne schválené daným jednotlivcom. Čo sa týka citlivých údajov, „jednotlivcom musí byť poskytnutá možnosť potvrdzujúcej alebo explicitnej voľby (možnosť vyjadriť súhlas), ak sa príslušné informácie majú poskytnúť tretej strane alebo využiť na účel iný ako ten, na základe ktorého boli tieto informácie pôvodne zhromaždené alebo následne schválené jednotlivcom prostredníctvom výkonu voľby v zmysle vyjadrenia súhlasu“ [9];

— pravidlá týkajúce sa ďalšieho prenosu údajov – „aby mohli organizácie poskytnúť informácie tretej strane, musia uplatniť zásady oznámenia a možnosti voľby“ [10];

— pokiaľ ide o bezpečnosť údajov, povinnosť „organizáci[í] zakladajúc[ich], uchovávajúc[ich], využívajúc[ich] alebo rozširujúc[ich] osobné informácie… uskutočniť primerané preventívne opatrenia, aby vo vzťahu k týmto informáciám zabránili ich strate, zneužívaniu a neoprávnenému prístupu k nim, ich odhaľovaniu, zmene a zničeniu“ [11];

— pokiaľ ide o integritu údajov, povinnosť organizácií „prijať náležité opatrenia na zabezpečenie toho, že údaje sú spoľahlivé vo vzťahu k ich zamýšľanému využitiu, že sú presné, úplné a aktuálne“ [12];

— že jednotlivec, ktorého údaje uchováva určitá organizácia, musí v zásade „mať prístup k [týmto] informáciám… a… mať možnosť opraviť, zmeniť a doplniť alebo vypustiť určité informácie tam, kde sú tieto nepresné“ [13];

— povinnosť vytvoriť „mechanizmy zabezpečujúce dodržiavanie zásad, možnosť nápravy pre jednotlivcov, ktorých sa údaje týkajú a ktorí sú postihnutí v dôsledku nedodržiavania zásad a zabezpečujúce vyvodenie dôsledkov pre príslušnú organizáciu v prípade nedodržiavania zásad“ [14].

8 — Pozri prílohu I oddiel „Oznámenie“.

9 — Pozri prílohu I oddiel „Možnosť voľby“.

10 — Pozri prílohu I oddiel „Ďalší prenos“.

11 — Pozri prílohu I oddiel „Bezpečnosť“.

12 — Pozri prílohu I oddiel „Integrita údajov“.

13 — Pozri prílohu I oddiel „Prístup“.

14 — Pozri prílohu I oddiel „Vymáhanie výkonu“.

17. Organizácia so sídlom v Spojených štátoch, ktorá chce dodržiavať zásady bezpečného prístavu, je povinná stanoviť vo svojej stratégii ochrany súkromia, že verejne vyhlasuje, že sa zaväzuje dodržiavať tieto zásady a že ich skutočne dodržiava, a vykonať samocertifikáciu tým, že ministerstvu obchodu Spojených štátov oznámi, že dodržiava uvedené zásady. [15]

18. Organizácie môžu dodržiavať zásady bezpečného prístavu viacerými spôsobmi. Môžu sa napríklad „pripoj[iť] k samoregulačnému programu ochrany súkromia, ktorý je v súlade so zásadami, [alebo] splniť kritériá bezpečného prístavu aj tak, že vypracujú svoje vlastné samoregulačné stratégie ochrany súkromia, pokiaľ sú tieto v súlade so zásadami. … Navyše, organizácie podliehajúce zákonnému, regulačnému, administratívnemu alebo inému súboru právnych noriem (alebo súboru pravidiel) účinne ochraňujúcemu súkromie jednotlivcov môžu tiež spĺňať kritériá na získanie výhod vyplývajúcich zo štatútu ‚bezpečného prístavu'" [16].

19. Existuje niekoľko mechanizmov na kontrolu dodržiavania zásad bezpečného prístavu, ktoré kombinujú súkromnú arbitráž a dohľad orgánov verejnej moci. Kontrolu možno zabezpečiť prostredníctvom systému mimosúdneho urovnávania sporov nezávislou treťou osobou. Podniky sa navyše môžu zaviazať, že budú spolupracovať s výborom Únie pre ochranu údajov. Napokon Federálna obchodná komisia (Federal Trade Commission, ďalej len „FTC") na základe právomocí, ktoré jej priznáva článok 5 zákona o Federálnej obchodnej komisii (Federal Trade Commission Act), a ministerstvo dopravy (Department of Transportation) na základe právomocí, ktoré mu priznáva článok 41712 zákonníka Spojených štátov (United States Code) v hlave 49 tohto zákonníka, majú právomoc vybavovať sťažnosti.

20. Podľa štvrtého odseku prílohy I rozhodnutia 2000/520 dodržiavanie zásad bezpečného prístavu môže byť obmedzené okrem iného „na mieru potrebnú na splnenie požiadaviek národnej bezpečnosti, verejného záujmu alebo vymáhania práva" a „zákonmi, nariadeniami vlády alebo precedenčným právom, ktoré ustanovujú protichodné povinnosti alebo výslovné oprávnenia, za predpokladu, že pri vykonávaní každého takéhoto oprávnenia môže organizácia preukázať, že jej nedodržiavanie zásad je obmedzené do tej miery, ktorá je potrebná na splnenie vyššie stojacich legitímnych záujmov vyplývajúcich z takéhoto oprávnenia" [17].

21. Okrem toho možnosť príslušných orgánov členských štátov pozastaviť toky údajov podlieha viacerým podmienkam, ktoré sú uvedené v článku 3 ods. 1 rozhodnutia 2000/520.

22. Z prejednávaného návrhu na začatie prejudiciálneho konania vyplývajú otázky týkajúce sa rozsahu pôsobnosti rozhodnutia 2000/520 so zreteľom na články 7, 8 a 47 Charty základných práv Európskej únie (ďalej len la „Charta"), ako aj článok 25 ods. 6 a článok 28 smernice 95/46. Tento návrh bol podaný v konaní, ktorého účastníkmi sú pán Schrems a Data Protection Commissioner (dozorný úradník pre ochranu údajov, ďalej len „dozorný úradník") a ktorého predmetom je rozhodnutie dozorného úradníka neprešetriť sťažnosť podanú pánom Schremsom z dôvodu, že Facebook Ireland Ltd (ďalej len „Facebook Ireland") uchováva osobné údaje svojich používateľov na serveroch nachádzajúcich sa v Spojených štátoch.

23. Pán Schrems je rakúsky štátny príslušník a má bydlisko v Rakúsku. Od roku 2008 je používateľom sociálnej siete Facebook.

15 — Článok 1 ods. 2 a 3 rozhodnutia 2000/520. Pozri tiež prílohu II FAQ 6.

16 — Tretí odsek prílohy I.

17 — Pozri tiež časť B prílohy IV.

24. Všetci používatelia sociálnej siete Facebook, ktorí majú bydlisko na území Únie, musia uzavrieť zmluvu so spoločnosťou Facebook Ireland, ktorá je dcérskou spoločnosťou materskej spoločnosti Facebook Inc. so sídlom v Spojených štátoch (ďalej len „Facebook USA“). Niektoré alebo všetky údaje týkajúce sa klientov spoločnosti Facebook Ireland s bydliskom na území Únie sa prenášajú na servery spoločnosti USA, ktoré sa nachádzajú na území Spojených štátov, kde sa uchovávajú.

25. Pán Schrems predložil 25. júna 2013 dozornému úradníkovi sťažnosť, v ktorej v podstate tvrdil, že podľa práva a praxe Spojených štátov neexistuje s ohľadom na údaje uchovávané na území Spojených štátov žiadna skutočná ochrana pred sledovaním zo strany štátu. Vyplýva to z zistení, ku ktorým dospel pán Snowden od mája 2013 v súvislosti s činnosťami amerických spravodajských služieb, najmä National Security Agency (Národná bezpečnostná agentúra, ďalej len „NSA“).

26. Z týchto zistení najmä vyplýva, že NSA vytvorila program nazvaný „PRISM“, v rámci ktorého táto agentúra získala neobmedzený prístup k masovým údajom uchovávaným na serveroch nachádzajúcich sa v Spojených štátoch, ktoré vlastní alebo ovláda skupina spoločností pôsobiacich v oblasti internetu a technológií, ako je Facebook USA.

27. Dozorný úradník konštatoval, že nie je povinný prešetriť sťažnosť, keďže sťažnosť nemala právny základ. Uviedol, že neexistujú dôkazy o tom, že NSA získala prístup k údajom pána Schremsa. Okrem toho bolo podľa jeho názoru potrebné zamietnuť sťažnosť vzhľadom na rozhodnutie 2000/520, ktorým Komisia konštatovala, že Spojené štáty v rámci režimu bezpečného prístavu zabezpečujú primeranú úroveň ochrany prenášaných osobných údajov. Akákoľvek otázka týkajúca sa primeranosti ochrany týchto údajov v Spojených štátoch sa mala vyriešiť v súlade s týmto rozhodnutím, ktoré mu bránilo v preskúmaní problému, na ktorý poukázala sťažnosť.

28. Dozorný úradník zamietol sťažnosť na základe nasledujúcich vnútroštátnych predpisov.

29. Článok 10 ods. 1 zákona o ochrane údajov z roku 1988 (Data Protection Act 1988), zmeneného a doplneného zákonom (novelou) o ochrane údajov z roku 2003 [Data Protection (Amendment) Act 2003, ďalej len „zákon o ochrane údajov“], priznáva dozornému úradníkovi právomoc skúmať sťažnosti a stanovuje:

„a) Dozorný úradník môže prešetriť alebo dať prešetriť, či došlo, dochádza alebo hrozí, že dôjde k porušeniu ktorékoľvek z ustanovení tohto zákona v súvislosti s jednotlivcom bez ohľadu na to, či mu tento jednotlivec predloží sťažnosť pre porušenie ktoréhokoľvek z týchto ustanovení, alebo dozorný úradník inak dospeje k záveru, že mohlo alebo môže dôjsť k takému porušeniu.

b) Ak sa dozornému úradníkovi predloží sťažnosť podľa písmena a) tohto odseku, dozorný úradník

i) prešetrí alebo dá prešetriť sťažnosť, pokiaľ nedospeje k záveru, že je šikanózna alebo zneužívajúca, a

ii) ak sa mu v primeranej lehote nepodarí dosiahnuť zmier dotknutých subjektov vo veci, ktorá je predmetom sťažnosti, písomne upovedomí sťažovateľa o svojom rozhodnutí o sťažnosti a o tom, že sťažovateľ môže v prípade, ak toto rozhodnutie nepriaznivo zasahuje do jeho právneho postavenia, podať proti nemu žalobu podľa článku 26 tohto zákona do 21 dní od doručenia upovedomenia.“

30. V prejednávanom prípade dozorný úradník dospel k záveru, že sťažnosť pána Schremsa je „šikanózna alebo zneužívajúca“ v tom zmysle, že nemohla uspieť, lebo nemala právny základ. Z tohto dôvodu ju dozorný úradník odmietol prešetriť.

31. Článok 11 zákona o ochrane údajov upravuje prenos osobných údajov do zahraničia. Článok 11 ods. 2 písm. a) tohto zákona stanovuje:

„Ak v akomkoľvek konaní podľa tohto zákona vznikne otázka

i) či krajina alebo územie mimo Európskeho hospodárskeho priestoru [(EHP)], do ktorého sa majú osobné údaje preniesť, zabezpečuje primeranú úroveň ochrany v zmysle odseku 1 tohto článku, a

ii) v súvislosti s dotknutým druhom prenosov sa dospelo ku konštatovaniu Spoločenstva,

otázka sa vyrieši v súlade s týmto konštatovaním."

32. Článok 11 ods. 2 písm. b) zákona o ochrane údajov vymedzuje pojem „konštatovanie Spoločenstva" takto:

„‚Konštatovanie Spoločenstva' v zmysle písmena a) tohto odseku znamená konštatovanie, ku ktorému dospela Európska komisia na účely článku 25 ods. 4 alebo 6 smernice [95/46] postupom podľa článku 31 ods. 2 [tejto smernice] s cieľom určiť, či krajina alebo územie mimo Európskeho hospodárskeho priestoru [(EHP)] zabezpečuje primeranú úroveň ochrany v zmysle odseku 1 tohto článku."

33. Dozorný úradník poznamenal, že rozhodnutie 2000/520 je „konštatovaním Spoločenstva" na účely článku 11 ods. 2 písm. a) zákona o ochrane údajov, takže podľa tohto zákona sa akákoľvek otázka týkajúca sa primeranosti ochrany údajov v tretej krajine, do ktorej sa údaje prenášajú, mala vyriešiť v súlade s týmto konštatovaním. Keďže toto bolo podstatou sťažnosti pána Schremsa – konkrétne že osobné údaje boli prenesené do tretej krajiny, ktorá v praxi nezabezpečovala primeranú úroveň ochrany – dozorný úradník dospel k záveru, že povaha a samotná existencia rozhodnutia 2000/520 mu bránia v preskúmaní tejto otázky.

34. Pán Schrems podal proti rozhodnutiu dozorného úradníka, ktorým bola jeho sťažnosť zamietnutá, žalobu na High Court. Tento súd po preskúmaní dôkazov predložených v konaní vo veci samej konštatoval, že elektronické sledovanie a zaznamenávanie osobných údajov zodpovedajú potrebným a nevyhnutným cieľom verejného záujmu, konkrétne ochrane národnej bezpečnosti a predchádzaniu závažnej trestnej činnosti. High Court v tejto súvislosti uvádza, že sledovanie a zaznamenávanie osobných údajov prenášaných z Únie do Spojených štátov slúži legitímnym cieľom súvisiacim s bojom proti terorizmu.

35. Podľa toho istého súdu zistenia, ku ktorým dospel pán Snowden, však ukázali, že NSA a iné podobné orgány v značnej miere prekročili svoje právomoci. Hoci Foreign Intelligence Surveillance Court (súd pre dohľad nad zahraničnými spravodajskými službami, ďalej len „FISC"), ktorý pôsobí na základe zákona o dohľade nad zahraničnými spravodajskými službami z roku 1978 (Foreign Intelligence Surveillance Act of 1978)[18], vykonáva dohľad, konanie na tomto súde je vždy tajné a nekontradiktórne. Okrem toho, že rozhodnutia týkajúce sa prístupu k osobným údajom sa prijímajú na základe práva Spojených štátov, občania Únie nemajú nijaké skutočné právo byť vypočutí v otázke sledovania a zaznamenávania svojich údajov.

18 — Pozri článok 702 tohto zákona, zmeneného a doplneného zákonom z roku 2008 (Foreign Intelligence Surveillance Act of 2008). Na základe tohto článku vedie NSA databázu známu pod názvom „PRISM" (pozri Report on the Findings by the EU Co-chairs of the ad hoc EU-US Working Group on Data Protection z 27. novembra 2013).

36. Z rozsiahlej dokumentácie pripojenej k prísažným vyhláseniam predloženým v konaní vo veci samej jasne vyplýva, že presnosť väčšiny zistení, ku ktorým dospel pán Snowden, je nesporná. High Court preto dospel k záveru, že NSA, ako aj iné bezpečnostné agentúry Spojených štátov, ako napríklad Federal Bureau of Investigation (Federálny úrad pre vyšetrovanie – FBI), môžu po prenose osobných údajov do Spojených štátov získať prístup k týmto údajom v rámci masového a nediferencovaného sledovania a zaznamenávania.

37. High Court konštatuje, že v írskom práve musí byť vzhľadom na význam ústavných práv na súkromie a nedotknuteľnosť obydlia každý zásah do týchto práv v súlade s požiadavkami stanovenými zákonom a musí byť primeraný. Masový a nediferencovaný prístup k osobným údajom vôbec nezodpovedá požiadavke proporcionality, a preto treba konštatovať, že je v rozpore s írskou ústavou. [19]

38. High Court poukazuje na to, že aby sa odpočúvanie elektronickej komunikácie mohlo považovať za ústavné, bolo by potrebné preukázať, že určité zaznamenávanie komunikácie a sledovanie určitých osôb alebo určitých skupín osôb je objektívne odôvodnené v záujme národnej bezpečnosti a boja proti trestnej činnosti a že existujú primerané a overiteľné záruky.

39. High Court preto uvádza, že ak by sa prejednávaná vec mala posúdiť výlučne podľa írskeho práva, vznikol by závažný problém, pokiaľ ide o to, či Spojené štáty „zaručujú primeranú úroveň ochrany súkromia a základných práv a slobôd“ v zmysle článku 11 ods. 1 zákona o ochrane údajov. Z toho vyplýva, že na základe írskeho práva, najmä jeho ústavných požiadaviek, dozorný úradník nemohol zamietnuť sťažnosť pána Schremsa, ale mal preskúmať túto otázku.

40. High Court však konštatuje, že vec, ktorú prejednáva, sa týka vykonávania práva Únie v zmysle článku 51 ods. 1 Charty, takže zákonnosť rozhodnutia dozorného úradníka by sa mala posúdiť z hľadiska práva Únie.

41. High Court vysvetlil problém, ktorému čelí dozorný úradník, takto. Podľa článku 11 ods. 2 písm. a) zákona o ochrane údajov je dozorný úradník povinný vyriešiť otázku primeranosti ochrany v tretej krajine „v súlade“ s konštatovaním Spoločenstva, ku ktorému dospela Komisia na základe článku 25 ods. 6 smernice 95/46. Z toho vyplýva, že dozorný úradník sa nemôže odchýliť od takého konštatovania. Keďže Komisia vo svojom rozhodnutí 2000/520 konštatovala, že Spojené štáty zaručujú primeranú úroveň ochrany, pokiaľ ide o spracovanie údajov spoločnosťami, ktoré dodržiavajú zásady bezpečného prístavu, dozorný úradník musí nevyhnutne zamietnuť sťažnosť, v ktorej sa namieta neprimeranosť takej ochrany.

42. Hoci High Court konštatuje, že dozorný úradník sa dôsledne pridŕžal znenia smernice 95/46 a rozhodnutia 2000/520, poukazuje na to, že výhrady pána Schremsa smerujú v skutočnosti skôr proti obsahu samotného režimu bezpečného prístavu než proti spôsobu, akým ho dozorný úradník uplatnil, pričom zdôrazňuje, že pán Schrems priamo nespochybnil platnosť smernice 95/46 ani platnosť rozhodnutia 2000/520.

43. Podľa High Court je teda rozhodujúcou otázkou, či je dozorný úradník so zreteľom na právo Únie a s prihliadnutím najmä na články 7 a 8 Charty, ktoré neskôr vstúpili do platnosti, absolútne viazaný konštatovaním Komisie o primeranosti práva a praxe Spojených štátov v oblasti ochrany osobných údajov, ktoré je uvedené v rozhodnutí 2000/520.

19 — High Court uvádza konkrétne rešpektovanie ľudskej dôstojnosti a slobody jednotlivca (preambula), osobnú nezávislosť (článok 40 ods. 3 body 1 a 2), nedotknuteľnosť obydlia (článok 40 ods. 5) a ochranu rodinného života (článok 41).

44. High Court navyše spresňuje, že v konaní na tomto súde vôbec nebola nastolená otázka týkajúca sa postupov spoločností Facebook Ireland a Facebook USA ako takých. Článok 3 ods. 1 písm. b) rozhodnutia 2000/520, ktorý dovoľuje príslušným vnútroštátnym orgánom nariadiť podniku, aby pozastavil toky údajov do tretej krajiny, sa pritom podľa tohto súdu uplatní len za okolností, keď sťažnosť smeruje proti konaniu dotknutého podniku, čo v prejednávanom prípade neplatí.

45. High Court preto zdôrazňuje, že skutočná výhrada nesmeruje proti konaniu spoločnosti Facebook USA ako takému, ale skôr proti tomu, že Komisia usúdila, že právo a prax Spojených štátov v oblasti ochrany údajov zaručujú primeranú ochranu, zatiaľ čo zistenia pána Snowdena jasne svedčia o tom, že orgány Spojených štátov môžu získať masový a nediferencovaný prístup k osobným údajom osôb s bydliskom na území Únie. [20]

46. V tejto súvislosti High Court uvádza, že je ťažké predstaviť si, ako by rozhodnutie 2000/520 mohlo v praxi spĺňať požiadavky článkov 7 a 8 Charty, najmä so zreteľom na zásady stanovené Súdnym dvorom v rozsudku Digital Rights Ireland a i. [21] Záruka stanovená článkom 7 Charty a základnými hodnotami spoločnými pre tradície členských štátov by konkrétne bola ohrozená, ak by orgány verejnej moci mohli náhodne a všeobecne získať prístup k elektronickej komunikácii bez toho, aby museli uviesť objektívne odôvodnenie založené na dôvodoch národnej bezpečnosti alebo predchádzania trestnej činnosti, ktoré špecificky súvisia s dotknutými jednotlivcami, a to bez akejkoľvek primeranej a overiteľnej záruky. Keďže zo žaloby pána Schremsa vyplýva, že rozhodnutie 2000/520 by mohlo byť *in abstracto* nezlučiteľné s článkami 7 a 8 Charty, Súdny dvor by mohol dospieť k záveru, že smernicu 95/46, najmä jej článok 25 ods. 6, ako aj rozhodnutie 2000/520 možno vykladať v tom zmysle, že vnútroštátne orgány môžu vykonať vlastné vyšetrovanie s cieľom určiť, či prenos osobných údajov do tretej krajiny a ich uchovávanie v tretej krajine zodpovedá požiadavkám vyplývajúcim z článkov 7 a 8 Charty.

47. Za týchto podmienok High Court rozhodol o prerušení konania a položil Súdnemu dvoru nasledujúce prejudiciálne otázky:

„Je [dozorný úradník] pri posudzovaní sťažnosti, ktorá mu bola predložená a ktorá sa týka toho, že osobné údaje sa prenášajú do tretej krajiny (v tomto prípade do Spojených štátov amerických), ktorej zákony a prax údajne neposkytujú dotknutej osobe primeranú ochranu, absolútne viazaný konštatovaním Spoločenstva uvedeným v [rozhodnutí 2000/520], ktoré znie v opačnom zmysle, a to vzhľadom na články 7, 8 a 47 [Charty] a bez toho, aby bol dotknutý článok 25 ods. 6 smernice [95/46]?

Alebo subsidiárne [dozorný úradník] môže a/alebo musí vykonať v tejto veci vlastné vyšetrovanie vzhľadom na vývoj skutkových okolností, ku ktorému došlo odvtedy, ako bolo [rozhodnutie 2000/520] prvýkrát uverejnené?“

II – **Moja analýza**

48. Na základe dvoch otázok, ktoré položil High Court, má Súdny dvor spresniť, akými právomocami disponujú vnútroštátne dozorné orgány pri posudzovaní sťažnosti týkajúcej sa prenosu osobných údajov do podniku so sídlom v tretej krajine, ak sa na podporu tejto sťažnosti uvádza, že príslušná tretia krajina nezaručuje primeranú úroveň ochrany prenášaných údajov, hoci Komisia na základe článku 25 ods. 6 smernice 95/46 prijala rozhodnutie, ktorým uznala primeranosť úrovne ochrany poskytovanej uvedenou treťou krajinou.

20 — High Court v tejto súvislosti uvádza, že kľúčový žalobný dôvod, ktorý pán Schrems uviedol vo svojej žalobe, spočíval v tvrdení, že vzhľadom na nedávne odhalenia pána Snowdena a na sprístupňovanie osobných údajov spravodajským službám Spojených štátov vo veľkom rozsahu dozorný úradník nemohol oprávnene dospieť k záveru, že v tejto tretej krajine existuje primeraná úroveň ochrany týchto údajov.

21 — C-293/12 a C-594/12, EU:C:2014:238, body 65 až 69.

49. Poznamenávam, že sťažnosť, ktorú pán Schrems predložil dozornému úradníkovi, má dva aspekty. Jej cieľom je napadnúť prenos osobných údajov zo spoločnosti Facebook Ireland do spoločnosti Facebook USA. Pán Schrems sa domáha ukončenia tohto prenosu, keďže Spojené štáty podľa jeho názoru nezabezpečujú primeranú úroveň ochrany osobných údajov, ktoré sa prenášajú v rámci režimu bezpečného prístavu. Presnejšie tejto tretej krajine vytýka, že zaviedla program PRISM, ktorý dovoľuje NSA získať neobmedzený prístup k masovým údajom uchovávaným na serveroch nachádzajúcich sa v Spojených štátoch. Sťažnosť sa teda týka konkrétne prenosov osobných údajov zo spoločnosti Facebook Ireland do spoločnosti Facebook USA, pričom všeobecnejšie spochybňuje úroveň ochrany takých údajov poskytovanú v rámci režimu bezpečného prístavu.

50. Dozorný úradník konštatoval, že samotná existencia rozhodnutia Komisie, ktorým sa uznáva, že Spojené štáty zaisťujú v rámci režimu bezpečného prístavu primeranú úroveň ochrany, mu bráni v prešetrení sťažnosti.

51. Obe otázky, ktorými sa vnútroštátny súd v podstate pýta, či sa má článok 28 smernice 95/46 v spojení s článkami 7 a 8 Charty vykladať v tom zmysle, že existencia rozhodnutia Komisie prijatého na základe článku 25 ods. 6 tejto smernice bráni vnútroštátnemu dozornému orgánu v tom, aby prešetril sťažnosť, v ktorej sa namieta, že tretia krajina nezabezpečuje primeranú úroveň ochrany prenášaných osobných údajov, a prípadne pozastavil prenos týchto údajov, teda treba preskúmať súčasne.

52. Článok 7 Charty zaručuje právo na rešpektovanie súkromia, zatiaľ čo jej článok 8 výslovne deklaruje právo na ochranu osobných údajov. Odseky 2 a 3 tohto posledného uvedeného článku spresňujú, že tieto údaje musia byť riadne spracované na určené účely na základe súhlasu dotknutej osoby alebo na inom oprávnenom základe ustanovenom zákonom, že každý má právo na prístup k zhromaždeným údajom, ktoré sa ho týkajú, a právo na ich opravu a že dodržiavanie týchto pravidiel podlieha kontrole nezávislého orgánu.

A – *O právomociach vnútroštátnych dozorných orgánov v prípade rozhodnutia o primeranosti prijatého Komisiou*

53. Ako pán Schrems uvádza vo svojich pripomienkach, kľúčovou otázkou sťažnosti, o ktorú ide v konaní vo veci samej, je otázka prenosu osobných údajov zo spoločnosti Facebook Ireland do spoločnosti Facebook USA vzhľadom na neobmedzený prístup NSA a iných bezpečnostných agentúr Spojených štátov k údajom uchovávaným v spoločnosti Facebook USA na základe právomocí, ktoré im priznávajú právne predpisy Spojených štátov.

54. Vnútroštátny dozorný orgán, ktorý rozhoduje o sťažnosti smerujúcej k spochybneniu konštatovania, že tretia krajina zaisťuje primeranú úroveň ochrany prenášaných údajov, má podľa pána Schremsa v prípade, ak má dôkazy, ktoré svedčia o dôvodnosti tvrdení uvedených v tejto sťažnosti, právomoc nariadiť pozastavenie prenosu údajov vykonávaného podnikom označeným v uvedenej sťažnosti.

55. Vzhľadom na povinnosti dozorného úradníka spočívajúce v ochrane jeho základných práv pán Schrems tvrdí, že dozorný úradník má povinnosť nielen prešetriť sťažnosť, ale v prípade, ak jej vyhovie, tiež využiť svoje právomoci na pozastavenie toku údajov medzi spoločnosťami Facebook Ireland a Facebook USA.

56. Dozorný úradník však zamietol sťažnosť na základe ustanovení zákona o ochrane údajov, v ktorých sú vymenované jeho právomoci. Tento záver bol založený na názore dozorného úradníka, že bol viazaný rozhodnutím 2000/520.

57. Z toho vyplýva, že základným problémom v prejednávanej veci je, či je posúdenie Komisie týkajúce sa primeranosti úrovne ochrany, ktoré je uvedené v rozhodnutí 2000/520, absolútne záväzné pre vnútroštátny orgán na ochranu údajov a bráni mu v prešetrení tvrdení smerujúcich k spochybneniu tohto konštatovania. Prejudiciálne otázky sa teda týkajú rozsahu vyšetrovacích právomocí vnútroštátnych orgánov na ochranu údajov v prípade rozhodnutia o primeranosti prijatého Komisiou.

58. Podľa Komisie treba vziať do úvahy rozdelenie právomocí medzi ňu a vnútroštátne orgány na ochranu údajov. Právomoci týchto orgánov sú zamerané na uplatňovanie právnych predpisov v tejto oblasti v individuálnych prípadoch, zatiaľ čo všeobecné preskúmanie uplatňovania rozhodnutia 2000/520, vrátane akéhokoľvek rozhodnutia, ktoré by viedlo k pozastaveniu jeho účinnosti alebo k jeho zrušeniu, spadá do právomoci Komisie.

59. Komisia tvrdí, že pán Schrems neuviedol konkrétne tvrdenia, z ktorých by vyplývalo, že mu bezprostredne hrozí vážna škoda v dôsledku prenosu údajov medzi spoločnosťami Facebook Ireland a Facebook USA. Obavy, ktoré pán Schrems vyjadril v súvislosti s programami sledovania zavedenými bezpečnostnými agentúrami Spojených štátov, sú naopak vzhľadom na ich abstraktnú a všeobecnú povahu totožné s obavami, na základe ktorých Komisia začala s revíziou rozhodnutia 2000/520.

60. Podľa Komisie by vnútroštátne dozorné orgány v prípade, ak by prijímali opatrenia na základe sťažností, v ktorých sú uvedené len systémové a abstraktné obavy, zasahovali do jej právomocí spočívajúcich v opätovnom prerokovaní podmienok tohto rozhodnutia so Spojenými štátmi alebo prípadne v pozastavení jeho účinnosti.

61. Nesúhlasím s názorom Komisie. Domnievam sa, že existencia rozhodnutia Komisie prijatého na základe článku 25 ods. 6 smernice 95/46 nemôže vylúčiť ani obmedziť právomoci, ktorými disponujú vnútroštátne dozorné orgány podľa článku 28 tejto smernice. V rozpore s tým, čo tvrdí Komisia, si vnútroštátne dozorné orgány podľa môjho názoru môžu v prípade, ak posudzujú individuálne sťažnosti, na základe svojich vyšetrovacích právomocí a svojej nezávislosti urobiť vlastný názor na všeobecnú úroveň ochrany, ktorú poskytuje tretia krajina, a vyvodiť z neho dôsledky pri rozhodovaní o individuálnych prípadoch.

62. Z ustálenej judikatúry Súdneho dvora vyplýva, že na účely výkladu určitého ustanovenia práva Únie treba zohľadniť nielen jeho znenie, ale aj jeho kontext a ciele sledované právnou úpravou, ktorej je súčasťou. [22]

63. Z odôvodnenia 62 smernice 95/46 vyplýva, že „zriadenie dozorných úradov v členských štátoch, ktoré vykonávajú svoje funkcie s úplnou nezávislosťou, je nevyhnutným komponentom ochrany jednotlivcov v súvislosti so spracovaním osobných údajov“.

64. Podľa článku 28 ods. 1 prvého pododseku tejto smernice „každý členský štát zabezpečí, aby jeden alebo viac štátnych orgánov bolo zodpovedných za monitorovanie uplatňovania ustanovení v rámci jeho územia, prijatých členskými štátmi v súlade s touto smernicou“. Článok 28 ods. 1 druhý pododsek uvedenej smernice stanovuje, že „tieto orgány konajú s úplnou nezávislosťou vo vykonávaní im zverených funkcií“.

65. V článku 28 ods. 3 smernice 95/46 sú vymenované právomoci každého dozorného orgánu, a to vyšetrovacie právomoci, efektívne právomoci intervencie, ktoré mu dovoľujú okrem iného dočasne alebo úplne zakázať spracovanie, ako aj právomoc podať návrh na začatie súdneho konania v prípade, ak došlo k porušeniu vnútroštátnych ustanovení prijatých v súlade s touto smernicou, alebo právomoc upozorniť súdne orgány na také porušenie.

22 — Pozri najmä rozsudok Koushkaki (C-84/12, EU:C:2013:862, bod 34 a citovanú judikatúru).

66. Okrem toho podľa článku 28 ods. 4 prvého pododseku smernice 95/46 „každý dozorný orgán si vypočuje nároky uplatňované každou osobou … týkajúce sa ochrany jeho práv a slobôd vzhľadom na spracovanie osobných údajov“. Článok 28 ods. 4 druhý pododsek tejto smernice spresňuje, že „každý dozorný orgán si vypočuje najmä nároky na kontrolu zákonnosti spracovania údajov, uplatnené každou osobou, keď sa uplatňujú vnútroštátne ustanovenia prijaté v súlade s článkom 13 tejto smernice“. Poznamenávam, že toto posledné uvedené ustanovenie dovoľuje členským štátom prijať legislatívne opatrenia na obmedzenie rozsahu viacerých povinností a práv uvedených v smernici 95/46, keď takéto obmedzenie predstavuje nevyhnutné opatrenie okrem iného na ochranu štátnej bezpečnosti, obrany, verejnej bezpečnosti, ako aj na predchádzanie, vyšetrovanie, odhaľovanie a stíhanie trestných činov.

67. Ako Súdny dvor už konštatoval, požiadavka kontroly nad dodržiavaním pravidiel Únie na ochranu fyzických osôb v súvislosti so spracovaním osobných údajov zo strany nezávislého orgánu vyplýva tiež z primárneho práva Únie, najmä z článku 8 ods. 3 Charty a z článku 16 ods. 2 ZFEÚ.[23] Tiež pripomenul, že „zriadenie nezávislých dozorných orgánov v členských štátoch tak predstavuje základný prvok ochrany osôb v súvislosti so spracovaním osobných údajov“[24].

68. Súdny dvor tiež rozhodol, že „článok 28 ods. 1 druhý pododsek smernice 95/46 sa má vykladať v tom zmysle, že dozorným orgánom povereným dohľadom nad spracovaním osobných údajov musí byť priznaná nezávislosť, ktorá im umožní vykonávať ich úlohy bez vonkajšieho vplyvu. Táto nezávislosť vylučuje najmä akýkoľvek príkaz či iný vonkajší vplyv v akejkoľvek forme, či už priamy, alebo nepriamy, ktorý by mohol ovplyvniť ich rozhodnutia a tým spochybniť vykonávanie úloh uvedenými orgánmi, ktoré spočívajú v zabezpečení spravodlivej rovnováhy medzi ochranou základného práva na súkromie a voľným pohybom osobných údajov“[25].

69. Súdny dvor tiež spresnil, že „záruka nezávislosti vnútroštátnych dozorných orgánov má zabezpečiť účinnosť a spoľahlivosť dohľadu nad dodržiavaním právnych predpisov v oblasti ochrany fyzických osôb pri spracovaní osobných údajov“[26]. Táto záruka nezávislosti bola vytvorená „s cieľom posilniť ochranu osôb a subjektov dotknutých… rozhodnutiami [týchto vnútroštátnych dozorných orgánov]“[27].

70. Ako vyplýva najmä z odôvodnenia 10 a z článku 1 smernice 95/46, táto smernica má za cieľ zabezpečiť v rámci Únie „vysokú úroveň ochrany základných práv a slobôd… pri spracovaní osobných údajov“[28]. Podľa Súdneho dvora „dozorné orgány uvedené v článku 28 smernice 95/46 sú teda strážcovia týchto základných práv a slobôd“[29].

71. Vzhľadom na význam úlohy vnútroštátnych dozorných orgánov v oblasti ochrany fyzických osôb pri spracovaní osobných údajov musia ich intervenčné právomoci zostať nedotknuté aj v prípade, ak Komisia prijala rozhodnutie na základe článku 25 ods. 6 smernice 95/46.

72. V tejto súvislosti poznamenávam, že nič nenasvedčuje tomu, že režimy prenosu osobných údajov do tretích krajín sú vylúčené z vecnej pôsobnosti článku 8 ods. 3 Charty, ktorý v rámci noriem najvyššej právnej sily v práve Únie zakotvuje význam kontroly vykonávanej nezávislým orgánom, pokiaľ ide o dodržiavanie pravidiel týkajúcich sa ochrany osobných údajov.

23 — Pozri rozsudky Komisia/Rakúsko (C-614/10, EU:C:2012:631, bod 36) a Komisia/Maďarsko (C-288/12, EU:C:2014:237, bod 47).

24 — Pozri najmä rozsudok Komisia/Maďarsko (C-288/12, EU:C:2014:237, bod 48 a citovanú judikatúru). Pozri v tomto zmysle tiež rozsudok Digital Rights Ireland a i. (C-293/12 a C-594/12, EU:C:2014:238, bod 68, ako aj citovanú judikatúru).

25 — Pozri najmä rozsudok Komisia/Maďarsko (C-288/12, EU:C:2014:237, bod 51 a citovanú judikatúru).

26 — Rozsudok Komisia/Nemecko (C-518/07, EU:C:2010:125, bod 25).

27 — Tamže.

28 — Tamže, bod 22 a citovaná judikatúra.

29 — Tamže, bod 23. Pozri v tomto zmysle tiež rozsudky Komisia/Rakúsko (C-614/10, EU:C:2012:631, bod 52) a Komisia/Maďarsko (C-288/12, EU:C:2014:237, bod 53).

73. Ak by vnútroštátne dozorné orgány boli absolútne viazané rozhodnutiami prijatými Komisiou, nevyhnutne by to obmedzovalo ich úplnú nezávislosť. Vnútroštátne dozorné orgány musia mať v súlade so svojou úlohou strážcov základných práv právomoc úplne nezávisle prešetriť sťažnosti, ktoré im boli predložené, vo vyššom záujme ochrany jednotlivcov pri spracovaní osobných údajov.

74. Okrem toho, ako belgická vláda a Európsky parlament správne poznamenali na pojednávaní, neexistuje nijaká hierarchická súvislosť medzi kapitolou IV smernice 95/46 týkajúcou sa prenosu osobných údajov do tretích krajín a jej kapitolou VI, ktorá sa týka okrem iného úlohy vnútroštátnych dozorných orgánov. Nič v tejto kapitole VI nenasvedčuje tomu, že ustanovenia týkajúce sa vnútroštátnych dozorných orgánov sú akokoľvek podriadené odlišným ustanoveniam týkajúcim sa prenosov uvedeným v kapitole IV smernice 95/46.

75. Z článku 25 ods. 1 tejto smernice, ktorý je súčasťou jej kapitoly IV, naopak výslovne vyplýva, že povolenie prenosu osobných údajov do tretej krajiny, ktorá zaisťuje primeranú úroveň ochrany, platí len za predpokladu, že budú dodržané vnútroštátne ustanovenia prijaté v súlade s ostatnými ustanoveniami tejto smernice.

76. V tomto smere pripomínam, že podľa tohto ustanovenia musia členské štáty vo svojich vnútroštátnych predpisoch stanoviť, že k prenosu osobných údajov, ktoré sa spracovávajú alebo sú určené na spracovanie po prenose, do tretej krajiny môže dôjsť len vtedy, ak – za predpokladu, že budú dodržané vnútroštátne ustanovenia prijaté v súlade s ostatnými ustanoveniami smernice 95/46 – príslušná tretia krajina zaistí primeranú úroveň ochrany týchto údajov.

77. Podľa článku 28 ods. 1 tejto smernice sú vnútroštátne dozorné orgány zodpovedné za monitorovanie uplatňovania ustanovení prijatých členskými štátmi v súlade s touto smernicou na území každého členského štátu.

78. Na základe porovnania týchto dvoch ustanovení možno konštatovať, že pravidlo stanovené v článku 25 ods. 1 smernice 95/46, podľa ktorého k prenosu osobných údajov môže dôjsť len vtedy, ak tretia krajina, do ktorej majú byť tieto údaje prenesené, zaistí primeranú úroveň ich ochrany, patrí medzi pravidlá, ktorých uplatňovanie majú vnútroštátne dozorné orgány monitorovať.

79. Právomoci vnútroštátnych dozorných orgánov úplne nezávisle prešetrovať sťažnosti, ktoré im boli predložené podľa článku 28 smernice 95/46, sa musia vykladať extenzívne, v súlade s článkom 8 ods. 3 Charty. Tieto právomoci teda nemôžu byť obmedzené právomocami, ktoré normotvorca Únie priznal Komisii podľa článku 25 ods. 6 tejto smernice na účely konštatovania primeranosti úrovne ochrany poskytovanej treťou krajinou.

80. Vzhľadom na svoju zásadnú úlohu v oblasti ochrany osobných údajov musia mať vnútroštátne dozorné orgány právomoc vykonať vyšetrovanie, ak im je predložená sťažnosť, v ktorej sú uvedené skutočnosti, ktoré by mohli spochybniť úroveň ochrany, ktorú zabezpečuje tretia krajina, a to aj v prípade, ak Komisia v rozhodnutí prijatom na základe článku 25 ods. 6 smernice 95/46 konštatovala, že príslušná tretia krajina zaisťuje primeranú úroveň ochrany.

81. Ak vnútroštátny dozorný orgán po skončení svojho vyšetrovania usúdi, že sporný prenos údajov narúša ochranu, ktorú treba poskytnúť občanom Únie v súvislosti so spracovaním ich údajov, má právomoc pozastaviť predmetný prenos údajov, a to bez ohľadu na všeobecné posúdenie, ktoré Komisia uviedla vo svojom rozhodnutí.

82. Je totiž nesporné, že – podľa článku 25 ods. 2 smernice 95/46 – sa primeranosť úrovne ochrany poskytovanej treťou krajinou posudzuje v závislosti od súboru skutkových, ako aj právnych okolností. Ak sa jedna z týchto okolností zmení a zdá sa, že môže spochybniť primeranosť úrovne ochrany poskytovanej treťou krajinou, vnútroštátny dozorný orgán, ktorému bola predložená sťažnosť, musí mať právomoc vyvodiť z toho dôsledky vo vzťahu k spornému prenosu.

83. Je pravda, že – ako poznamenalo Írsko – dozorný úradník je tak ako ostatné štátne orgány viazaný rozhodnutím 2000/520. Z článku 288 štvrtého odseku ZFEÚ totiž vyplýva, že rozhodnutie prijaté inštitúciou Únie je záväzné v celom rozsahu. Rozhodnutie 2000/520 preto zaväzuje členské štáty, ktorým je určené.

84. V tejto súvislosti poznamenávam, že samotné rozhodnutie 2000/520 v článku 5 stanovuje, že „členské štáty prijmú opatrenia potrebné na dosiahnutie súladu s týmto rozhodnutím najneskôr do uplynutia lehoty 90 dní odo dňa jeho oznámenia členským štátom“. Článok 6 tohto rozhodnutia navyše potvrdzuje, že „toto rozhodnutie je adresované členským štátom“.

85. Domnievam sa však, že vzhľadom na citované ustanovenia smernice 95/46 a Charty záväznosť rozhodnutia 2000/520 nemôže vylúčiť akékoľvek vyšetrovanie dozorného úradníka týkajúce sa sťažností, v ktorých sa uvádza, že prenosy osobných údajov do Spojených štátov v rámci tohto rozhodnutia neposkytujú potrebné záruky ochrany, ktoré vyžaduje právo Únie. Inak povedané, taká záväznosť nemôže znamenať, že každá sťažnosť tohto druhu sa musí odmietnuť, teda že sa musí zamietnuť okamžite a bez akéhokoľvek skúmania jej dôvodnosti.

86. Dodávam, že zo systematiky článku 25 smernice 95/46 navyše vyplýva, že ku konštatovaniu, že tretia krajina zaisťuje alebo nezaisťuje primeranú úroveň ochrany, môžu dospieť buď členské štáty, alebo k nemu môže dospieť Komisia. Ide teda o spoločnú právomoc.

87. Z článku 25 ods. 6 tejto smernice vyplýva, že pokiaľ Komisia konštatuje, že tretia krajina zaisťuje primeranú úroveň ochrany v zmysle článku 25 ods. 2 uvedenej smernice, členské štáty musia prijať opatrenia potrebné na dosiahnutie súladu s rozhodnutím Komisie.

88. Keďže dôsledkom takého rozhodnutia je, že umožňuje prenosy osobných údajov do tretej krajiny, ktorej úroveň ochrany Komisia považuje za primeranú, členské štáty musia v zásade dovoliť, aby podniky so sídlom na ich území vykonávali také prenosy.

89. Článok 25 smernice 95/46 však nepriznáva Komisii výlučnú právomoc, pokiaľ ide o konštatovanie primeranosti alebo neprimeranosti úrovne ochrany prenášaných osobných údajov. Systematika tohto článku svedčí o tom, že v tejto oblasti zohrávajú určitú úlohu aj členské štáty. Rozhodnutie Komisie má síce veľký význam pri zabezpečení jednotnosti podmienok prenosu platných v členských štátoch. Táto jednotnosť však môže trvať len za predpokladu, že toto konštatovanie nie je spochybnené.

90. Tvrdenie, že podmienky prenosu osobných údajov do tretej krajiny musia byť jednotné, podľa môjho názoru stráca svoju opodstatnenosť v situácii, o akú ide v konaní vo veci samej, kde je Komisia nielen informovaná o tom, že jej konštatovanie je predmetom kritiky, ale sama ho kritizuje a vedie rokovania s cieľom napraviť ho.

91. Posúdenie primeranosti alebo neprimeranosti úrovne ochrany poskytovanej treťou krajinou tiež môže viesť k spolupráci medzi členskými štátmi a Komisiou. Článok 25 ods. 3 smernice 95/46 v tejto súvislosti stanovuje, že „členské štáty a Komisia sa navzájom informujú o prípadoch, keď sa domnievajú, že tretia krajina nezabezpečuje adekvátnu úroveň ochrany v rámci znenia odseku 2“. Ako poznamenáva Parlament, jasne to svedčí o tom, že členské štáty a Komisia majú zohrávať rovnocennú úlohu pri určovaní prípadov, v ktorých tretia krajina nezabezpečuje primeranú úroveň ochrany.

92. Účelom rozhodnutia o primeranosti je povoliť prenos osobných údajov do príslušnej tretej krajiny. To neznamená, že občania Únie sa už nemôžu obrátiť na dozorné orgány so žiadosťou o ochranu svojich osobných údajov. V tomto smere poznamenávam, že článok 28 ods. 4 prvý pododsek smernice 95/46, podľa ktorého „každý dozorný orgán [posúdi] nároky uplatňované každou osobou… týkajúce sa ochrany [jej] práv a slobôd vzhľadom na spracovanie osobných údajov“, nestanovuje výnimku z tejto zásady v prípade, ak Komisia prijala rozhodnutie na základe článku 25 ods. 6 tejto smernice.

93. Hoci teda rozhodnutie prijaté Komisiou na základe vykonávacích právomocí, ktoré jej priznáva toto posledné uvedené ustanovenie, znamená, že je povolený prenos osobných údajov do tretej krajiny, také rozhodnutie nemôže zbaviť členské štáty, najmä ich vnútroštátne dozorné orgány, všetkej právomoci a dokonca ani obmedziť ich oprávnenia, pokiaľ majú posúdiť tvrdenia týkajúce sa porušovania základných práv.

94. Vnútroštátny dozorný orgán musí byť schopný vykonávať právomoci uvedené v článku 28 ods. 3 smernice 95/46, vrátane právomoci dočasne alebo úplne zakázať spracovanie osobných údajov. Hoci vo výpočte právomocí, ktorý sa nachádza v tomto ustanovení, nie sú výslovne uvedené právomoci týkajúce sa prenosu z členského štátu do tretej krajiny, taký prenos treba podľa môjho názoru považovať za spracovanie údajov. [30] Ako vyplýva zo znenia tohto ustanovenia, tento výpočet navyše nie je taxatívny. V každom prípade vzhľadom na zásadnú úlohu, ktorú vnútroštátne dozorné orgány zohrávajú v systéme vytvorenom smernicou 95/46, tieto orgány musia mať právomoc pozastaviť prenos údajov v prípade, ak sa preukáže porušenie základných práv alebo ak hrozí ich porušenie.

95. Dodávam, že ak by bol vnútroštátny dozorný orgán za okolností, o aké ide v prejednávanej veci, zbavený svojich vyšetrovacích právomocí, bolo by to v rozpore nielen so zásadou nezávislosti, ale aj s cieľom smernice 95/46, ktorý vyplýva z článku 1 ods. 1 tejto smernice.

96. Ako poznamenal Súdny dvor, „z odôvodnení 3, 8 a 10 smernice 95/46 vyplýva, že normotvorca Únie mal v úmysle uľahčiť voľný pohyb osobných údajov aproximáciou právnych poriadkov členských štátov a súčasne chrániť základné práva osôb, najmä právo na ochranu súkromného života, a zaistiť vysokú úroveň ochrany v Únii. Článok 1 tejto smernice ukladá členským štátom povinnosť, aby v súvislosti so spracovávaním osobných údajov zabezpečili ochranu základných práv a slobôd fyzických osôb, najmä ich právo na súkromie“ [31].

97. Ustanovenia smernice 95/46 sa teda majú vykladať v súlade s cieľom tejto smernice, ktorým je zaistiť vysokú úroveň ochrany základných práv a slobôd fyzických osôb, najmä ich právo na súkromie, v súvislosti so spracovávaním osobných údajov v rámci Únie.

98. Z významu tohto cieľa a z úlohy, ktorú majú členské štáty zohrávať pri jeho dosahovaní, vyplýva, že ak osobitné okolnosti vyvolávajú vážnu pochybnosť o dodržiavaní základných práv zaručených Chartou v prípade prenosu osobných údajov do tretej krajiny, členské štáty, a teda ani ich vnútroštátne dozorné orgány nemôžu byť absolútne viazané rozhodnutím o primeranosti prijatým Komisiou.

99. Súdny dvor už rozhodol, že „ustanovenia smernice 95/46 sa majú v rozsahu, v akom upravujú spracovanie osobných údajov, ktoré môže viesť k porušeniu základných slobôd a predovšetkým práva na súkromie, nevyhnutne vykladať s prihliadnutím na základné práva, ktoré podľa ustálenej judikatúry tvoria súčasť všeobecných právnych zásad, ktorých dodržiavanie Súdny dvor zabezpečuje a ktoré sú v súčasnosti zapísané v Charte“ [32].

100. Poukazujem navyše na judikatúru, podľa ktorej „je povinnosťou členských štátov nielen vykladať ich vnútroštátne právo v súlade s právom Únie, ale tiež dohliadať na to, aby sa nevychádzalo z výkladu textu sekundárneho práva, ktorý by bol v rozpore so základnými právami chránenými právnym poriadkom Únie alebo s inými všeobecnými zásadami práva Únie“ [33].

30 — Pozri návrhy, ktoré predniesol generálny advokát Léger vo veci Parlament/Rada a Komisia (C-317/04 a C-318/04, EU:C:2005:710, body 92 až 95). Pozri tiež rozsudok Parlament/Rada a Komisia (C-317/04 a C-318/04, EU:C:2006:346, bod 56).

31 — Pozri najmä rozsudok IPI (C-473/12, EU:C:2013:715, bod 28 a citovanú judikatúru).

32 — Pozri najmä rozsudok Google Spain a Google (C-131/12, EU:C:2014:317, bod 68 a citovanú judikatúru).

33 — Pozri najmä rozsudok N. S. a i. (C-411/10 a C-493/10, EU:C:2011:865, bod 77, ako aj citovanú judikatúru).

101. Súdny dvor vo svojom rozsudku N. S. a i.[34] rozhodol, že „uplatnenie nariadenia [(ES)] č. 343/2003[35] na základe nevyvrátiteľnej domnienky, že v členskom štáte, ktorý má za normálnych okolností právomoc posúdiť jeho žiadosť, budú dodržané základné práva žiadateľa o azyl, je nezlučiteľné s povinnosťou členských štátov vykladať a uplatňovať nariadenie č. 343/2003 spôsobom, ktorý je v súlade so základnými právami“[36].

102. V tomto smere Súdny dvor v súvislosti s postavením členských štátov ako bezpečných krajín pôvodu vo vzájomných vzťahoch, čo sa týka všetkých právnych a praktických otázok týkajúcich sa práva azylu, uznal, že sa musí predpokladať, že zaobchádzanie so žiadateľmi o azyl v každom členskom štáte je v súlade s požiadavkami Charty, s Dohovorom o právnom postavení utečencov, podpísaným v Ženeve 28. júla 1951[37], ako aj s Európskym dohovorom o ochrane ľudských práv a základných slobôd, podpísaným v Ríme 4. novembra 1950[38]. Súdny dvor však rozhodol, že „nemožno… vylúčiť, že fungovanie tohto systému sa bude v praxi potýkať s veľkými ťažkosťami v konkrétnom členskom štáte, takže bude existovať vážne nebezpečenstvo, že sa so žiadateľmi o azyl v prípade odovzdania do tohto členského štátu bude zaobchádzať spôsobom nezlučiteľným s ich základnými právami“[39].

103. Súdny dvor preto rozhodol, že „členským štátom vrátane vnútroštátnych súdov prislúcha, aby neodovzdali žiadateľa o azyl do ‚zodpovedného členského štátu‘ v zmysle nariadenia č. 343/2003, pokiaľ nemôžu ignorovať, že systémové zlyhania azylového konania a podmienok prijatia žiadateľov o azyl v tomto členskom štáte predstavujú vážne a preukázané dôvody domnievať sa, že žiadateľ bude vystavený skutočnému nebezpečenstvu neľudského alebo ponižujúceho zaobchádzania v zmysle článku 4 Charty“[40].

104. Domnievam sa, že pôsobnosť záverov vyplývajúcich z rozsudku N. S. a i.[41] možno rozšíriť aj na situáciu, o akú ide vo veci samej. Výklad sekundárneho práva Únie, ktorý spočíva na nevyvrátiteľnej domnienke, že budú dodržané základné práva – či už zo strany členského štátu, Komisie alebo tretej krajiny –, treba považovať za nezlučiteľný s povinnosťou členských štátov vykladať a uplatňovať sekundárne právo Únie spôsobom, ktorý je v súlade so základnými právami. Článok 25 ods. 6 smernice 95/46 teda nestanovuje takú nevyvrátiteľnú domnienku dodržiavania základných práv, pokiaľ ide o posúdenie Komisie týkajúce sa primeranosti úrovne ochrany poskytovanej treťou krajinou. Naopak domnienka, že pri prenose údajov do tretej krajiny sa dodržiavajú základné práva, o ktorú sa opiera toto ustanovenie, sa musí považovať za vyvrátiteľnú.[42] Uvedené ustanovenie by sa teda nemalo vykladať tak, že spochybňuje záruky uvedené najmä v článku 28 ods. 3 smernice 95/46 a v článku 8 ods. 3 Charty, ktoré sa týkajú ochrany a dodržiavania práva na ochranu osobných údajov.

105. Z uvedeného rozsudku teda vyvodzujem, že v prípade systémových zlyhaní zistených v tretej krajine, do ktorej sa prenášajú osobné údaje, členské štáty musia mať právomoc prijať opatrenia potrebné na ochranu základných práv zaručených článkami 7 a 8 Charty.

34 — C-411/10 a C-493/10, EU:C:2011:865.

35 — Nariadenie Rady z 18. februára 2003 ustanovujúce kritériá a mechanizmy na určenie členského štátu zodpovedného za posúdenie žiadosti o azyl podanej štátnym príslušníkom tretej krajiny v jednom z členských štátov (Ú. v. EÚ L 50, s. 1; Mim. vyd. 19/006, s. 109).

36 — Bod 99 tohto rozsudku.

37 — *Zbierka zmlúv Spojených národov*, zv. 189, s. 150, č. 2545 (1954).

38 — Pozri rozsudok N. S. a i. (C-411/10 a C-493/10, EU:C:2011:865, bod 80).

39 — Tamže, bod 81.

40 — Tamže, bod 94.

41 — C-411/10 a C-493/10, EU:C:2011:865.

42 — Bod 104 tohto rozsudku.

106. Ako navyše talianska vláda poznamenala vo svojich pripomienkach, prijatie rozhodnutia o primeranosti Komisiou nemôže mať za následok zníženie úrovne ochrany občanov Únie pri spracovaní ich údajov, ak dochádza k prenosu týchto údajov do tretej krajiny, v porovnaní s úrovňou ochrany, ktorá by sa poskytla týmto osobám, ak by sa ich údaje spracovávali v rámci Únie. Vnútroštátne dozorné orgány musia byť preto schopné zasiahnuť a vykonať svoje právomoci v súvislosti s prenosmi údajov do tretích krajín, ktorých sa týka rozhodnutie o primeranosti. V opačnom prípade by občania Únie boli chránení v menšej miere ako v prípade spracovania ich údajov v rámci Únie.

107. Jediným dôsledkom prijatia rozhodnutia Komisie na základe článku 25 ods. 6 smernice 95/46 je teda zrušenie všeobecného zákazu vývozu osobných údajov do tretích krajín, ktoré zaručujú úroveň ochrany porovnateľnú s úrovňou ochrany poskytovanou touto smernicou. Inak povedané, nejde o vytvorenie osobitného režimu výnimky, ktorý chráni občanov Únie v menšej miere ako všeobecný režim stanovený uvedenou smernicou pre spracovanie údajov v rámci Únie.

108. Je pravda, že Súdny dvor v bode 63 svojho rozsudku Lindqvist [43] uviedol, že „kapitola IV smernice 95/46, v ktorej sa nachádza článok 25, zavádza osobitný režim“. To však podľa môjho názoru neznamená, že taký režim musí poskytovať nižšiu úroveň ochrany. Naopak na dosiahnutie cieľa ochrany údajov uvedeného v článku 1 ods. 1 smernice 95/46 článok 25 tejto smernice ukladá členským štátom a Komisii rad povinností [44] a tento článok 25 stanovuje zásadu, že v prípade, ak tretia krajina neposkytuje primeranú úroveň ochrany, musí sa prenos osobných údajov do tejto krajiny zakázať [45].

109. Pokiaľ ide konkrétnejšie o režim bezpečného prístavu, Komisia počíta so zásahom vnútroštátnych dozorných orgánov a s tým, že tieto orgány pozastavia toky údajov len v rámci vymedzenom v článku 3 ods. 1 písm. b) rozhodnutia 2000/520.

110. Podľa odôvodnenia 8 tohto rozhodnutia „v záujme transparentnosti a s cieľom zabezpečenia schopnosti príslušných orgánov v členských štátoch zaručiť ochranu jednotlivcov v súvislosti so spracúvaním ich osobných údajov je potrebné, aby sa v tomto rozhodnutí presne vymedzili mimoriadne okolnosti, za ktorých by malo byť opodstatnené pozastavenie tokov určitých informácií, a to bez ohľadu na to, či Komisia prišla k záveru, že v danej krajine je zabezpečená primeraná úroveň ochrany“.

111. V rámci prejednávanej veci sa diskutovalo konkrétnejšie o uplatňovaní článku 3 ods. 1 písm. b) uvedeného rozhodnutia. Podľa tohto ustanovenia môžu vnútroštátne dozorné orgány rozhodnúť o pozastavení tokov údajov v prípadoch, keď „je veľká pravdepodobnosť, že sa porušujú zásady; existuje reálny dôvod na domnienku, že príslušný mechanizmus na vymáhanie výkonu neprijíma alebo neprijme primerané a včasné opatrenia na urovnanie určitého prípadu; pokračujúci prenos údajov by mal za následok bezprostredné riziko vážneho poškodenia dotknutých osôb, ktoré sú predmetom údajov; a príslušné orgány v danom členskom štáte vyvinuli podľa okolností primerané úsilie na to, aby o tom informovali dotknutú organizáciu a poskytli jej možnosť odpovedať“.

112. Uvedené ustanovenie stanovuje viaceré podmienky, ktoré účastníci konania počas tohto konania vyložili rôzne. [46] Bez toho, aby som sa podrobne zaoberal týmito výkladmi, vyplýva z nich, že tieto podmienky prísne obmedzujú právomoc vnútroštátnych dozorných orgánov pozastaviť toky údajov.

43 — C-101/01, EU:C:2003:596.

44 — Bod 65.

45 — Bod 64.

46 — Podľa pána Schremsa prvá podmienka, že „je veľká pravdepodobnosť, že sa porušujú zásady“, nie je splnená. Netvrdí sa, že Facebook USA ako samocertifikovaný subjekt, do ktorého sa prenášajú údaje, sám porušil zásady bezpečného prístavu z dôvodu masového a nediferencovaného prístupu orgánov Spojených štátov k údajom, ktoré uchováva. Zásady bezpečného prístavu sú totiž výslovne obmedzené právom Spojených štátov, ktoré je v štvrtom odseku prílohy I rozhodnutia 2000/520 vymedzené na základe zákonov, nariadení vlády a precedenčného práva.

113. V rozpore s tým, čo tvrdí Komisia, sa však článok 3 ods. 1 písm. b) rozhodnutia 2000/520 má vykladať v súlade s cieľom ochrany osobných údajov, ktorý sleduje smernica 95/46, ako aj z hľadiska článku 8 Charty. Požiadavka výkladu v súlade so základnými právami podporuje extenzívny výklad tohto ustanovenia.

114. Z toho vyplýva, že podmienky, ktoré sú stanovené v článku 3 ods. 1 písm. b) rozhodnutia 2000/520, nemôžu podľa môjho názoru brániť vnútroštátnemu dozornému orgánu v tom, aby úplne nezávisle vykonal právomoci, ktoré mu priznáva článok 28 ods. 3 smernice 95/46.

115. Ako belgická a rakúska vláda v podstate uviedli na pojednávaní, núdzové riešenie, ktoré poskytuje článok 3 ods. 1 písm. b) rozhodnutia 2000/520, je také obmedzené, že je ťažké zrealizovať ho v praxi. Toto riešenie vyžaduje splnenie kumulatívnych kritérií a stavia latku príliš vysoko. Z hľadiska článku 8 ods. 3 Charty je pritom vylúčené, aby manévrovací priestor vnútroštátnych dozorných orgánov, pokiaľ ide o právomoci vyplývajúce z článku 28 ods. 3 smernice 95/46, bol obmedzený do takej miery, že tieto právomoci už nemožno vykonať.

116. V tejto súvislosti Parlament správne poznamenal, že práve normotvorca Únie rozhodol, ktoré právomoci majú pripadnúť vnútroštátnym dozorným orgánom. Vykonávacia právomoc, ktorú normotvorca Únie priznal Komisii v článku 25 ods. 6 smernice 95/46, sa pritom nedotýka právomocí, ktoré ten istý normotvorca priznal v článku 28 ods. 3 tejto smernice vnútroštátnym dozorným orgánom. Inak povedané, Komisia nemá právomoc obmedziť právomoci vnútroštátnych dozorných orgánov.

117. Aby bola zabezpečená primeraná ochrana základných práv fyzických osôb pri spracovaní osobných údajov, vnútroštátne dozorné orgány teda musia byť oprávnené vykonať vyšetrovanie v prípade tvrdení, v ktorých sa namieta porušovanie týchto práv. Ak tieto orgány po skončení takého vyšetrovania dospejú k záveru, že v tretej krajine, na ktorú sa vzťahuje rozhodnutie o primeranosti, existujú vážne indície o porušovaní práva občanov Únie na ochranu ich osobných údajov, musia mať právomoc pozastaviť prenos údajov príjemcovi so sídlom v tejto tretej krajine.

118. Inak povedané, vnútroštátne dozorné orgány musia mať právomoc vykonať vyšetrovanie a prípadne pozastaviť prenos údajov bez ohľadu na reštriktívne podmienky stanovené v článku 3 ods. 1 písm. b) rozhodnutia 2000/520.

119. Okrem toho vnútroštátne dozorné orgány by na základe svojej právomoci podať návrh na začatie súdneho konania v prípade, ak došlo k porušeniu vnútroštátnych ustanovení prijatých v súlade so smernicou 95/46, alebo svojej právomoci upozorniť súdne orgány na také porušenie, ktoré sú stanovené v článku 28 ods. 3 tejto smernice, mali byť oprávnené – ak vedia o skutočnostiach, ktoré preukazujú, že tretia krajina nezabezpečuje primeranú úroveň ochrany – obrátiť sa na vnútroštátny súd, ktorý bude môcť sám prípadne rozhodnúť o podaní návrhu na začatie prejudiciálneho konania na Súdny dvor na účely posúdenia platnosti rozhodnutia o primeranosti prijatého Komisiou.

120. Zo všetkých týchto skutočností vyplýva, že článok 28 smernice 95/46 v spojení s článkami 7 a 8 Charty sa má vykladať v tom zmysle, že existencia rozhodnutia Komisie prijatého na základe článku 25 ods. 6 tejto smernice nebráni vnútroštátnemu dozornému orgánu v tom, aby prešetril sťažnosť, v ktorej sa uvádza, že tretia krajina nezabezpečuje primeranú úroveň ochrany prenášaných osobných údajov, a prípadne pozastavil prenos týchto údajov.

121. Hoci High Court vo svojom návrhu na začatie prejudiciálneho konania zdôrazňuje, že pán Schrems v konaní vo veci samej formálne nespochybnil platnosť smernice 95/46 ani platnosť rozhodnutia 2000/520, z tohto návrhu na začatie prejudiciálneho konania vyplýva, že cieľom hlavnej výhrady uvedenej pánom Schremsom je spochybniť konštatovanie, že Spojené štáty zabezpečujú v rámci režimu bezpečného prístavu primeranú úroveň ochrany prenášaných osobných údajov.

122. Z pripomienok dozorného úradníka tiež vyplýva, že cieľom sťažnosti pána Schremsa je priamo spochybniť rozhodnutie 2000/520. Pán Schrems chcel podaním tejto sťažnosti napadnúť podmienky a fungovanie režimu bezpečného prístavu ako takého z dôvodu, že masové sledovanie osobných údajov prenášaných do Spojených štátov svedčí o tom, že podľa práva a praxe tejto tretej krajiny neexistuje skutočná ochrana týchto údajov.

123. Vnútroštátny súd navyše sám poznamenáva, že záruka poskytovaná článkom 7 Charty a základnými hodnotami spoločnými pre ústavné tradície členských štátov by bola ohrozená, ak by orgány verejnej moci mohli náhodne a všeobecne získať prístup k elektronickej komunikácii bez toho, aby museli uviesť objektívne odôvodnenie založené na dôvodoch národnej bezpečnosti alebo predchádzania trestnej činnosti, ktoré špecificky súvisia s dotknutými jednotlivcami, a to bez akejkoľvek primeranej a overiteľnej záruky.[47] Vnútroštátny súd teda nepriamo pochybuje o platnosti rozhodnutia 2000/520.

124. Na posúdenie otázky, či Spojené štáty v rámci režimu bezpečného prístavu zaručujú primeranú úroveň ochrany prenášaných osobných údajov, je teda nevyhnutné zaoberať sa platnosťou tohto rozhodnutia.

125. V tejto súvislosti treba poukázať na to, že aj v prípade, ak sa návrh na začatie prejudiciálneho konania týka len otázky výkladu práva Únie, Súdny dvor môže v rámci nástroja spolupráce medzi ním a vnútroštátnymi súdmi, zavedeného článkom 267 ZFEÚ, za určitých okolností preskúmať platnosť ustanovení sekundárneho práva.

126. Súdny dvor preto viackrát *ex offo* vyhlásil určitý akt za neplatný, hoci vnútroštátny súd ho požiadal len o výklad toho aktu.[48] Tiež rozhodol, že, „keď sa zdá, že skutočný predmet otázok, ktoré položil vnútroštátny súd, sa týka skôr preskúmania platnosti než výkladu aktov [Únie], Súdny dvor má ihneď informovať tento súd o svojom názore bez toho, aby od neho vyžadoval splnenie formálnych požiadaviek vedúcich iba k prieťahom, ktoré sú nezlučiteľné so samotnou povahou mechanizmov zavedených článkom [267 ZFEÚ]“[49]. Súdny dvor navyše už konštatoval, že pochybnosti o zlučiteľnosti aktu sekundárneho práva s pravidlami týkajúcimi sa ochrany základných práv, ktoré vyjadril vnútroštátny súd, treba chápať tak, že spochybňujú platnosť tohto aktu z hľadiska práva Únie.[50]

127. Tiež pripomínam, že z judikatúry Súdneho dvora vyplýva, že pri aktoch inštitúcií a orgánov Únie platí prezumpcia platnosti, čo znamená, že také akty majú právne účinky dovtedy, kým neboli zrušené orgánom, ktorý ich prijal, zrušené na základe žaloby o neplatnosť alebo vyhlásené za neplatné v dôsledku návrhu na začatie prejudiciálneho konania alebo námietky nezákonnosti. Súdny dvor je výlučne príslušný na konštatovanie neplatnosti aktu Únie, čo má za cieľ zaručovať právnu istotu zabezpečením jednotného uplatnenia práva Únie. Pri absencii vyhlásenia neplatnosti, zmeny alebo zrušenia zo strany Komisie rozhodnutie zostáva záväzným vo všetkých bodoch a priamo uplatniteľným v každom členskom štáte.[51]

128. Zastávam názor, že s cieľom poskytnúť úplnú odpoveď vnútroštátnemu súdu a odstrániť pochybnosti o platnosti rozhodnutia 2000/520 vyjadrené počas tohto konania by mal Súdny dvor posúdiť platnosť tohto rozhodnutia.

47 — Bod 24 rozhodnutia vnútroštátneho súdu.

48 — Pozri najmä rozsudky Strehl (62/76, EU:C:1977:18, body 10 až 17), Roquette Frères (145/79, EU:C:1980:234, bod 6), ako aj Schutzverband der Spirituosen-Industrie (C-457/05, EU:C:2007:576, body 32 až 39).

49 — Rozsudok Schwarze (16/65, EU:C:1965:117, s. 1094).

50 — Pozri rozsudok Hauer (44/79, EU:C:1979:290, bod 16).

51 — Pozri najmä rozsudok CIVAD (C-533/10, EU:C:2012:347, body 39 až 41 a citovanú judikatúru).

129. Treba však tiež spresniť, že preskúmanie otázky, či rozhodnutie 2000/520 je alebo nie je platné, musí byť obmedzené na výhrady, ktoré boli predmetom rozpravy v rámci tohto konania. V rámci neho sa totiž nediskutovalo o všetkých aspektoch týkajúcich sa fungovania režimu bezpečného prístavu, a preto sa domnievam, že sa tu nemôžem venovať vyčerpávajúcemu skúmaniu nedostatkov tohto režimu.

130. Naopak otázka, či všeobecný a nediferencovaný prístup spravodajských služieb Spojených štátov k prenášaným údajom môže ovplyvniť zákonnosť rozhodnutia 2000/520, bola predmetom rozpravy na Súdnom dvore v rámci tohto konania. Platnosť tohto rozhodnutia teda možno posúdiť z tohto hľadiska.

B – *O platnosti rozhodnutia 2000/520*

1. O okolnostiach, ktoré treba vziať do úvahy pri posudzovaní platnosti rozhodnutia 2000/520

131. Treba pripomenúť judikatúru, podľa ktorej „v rámci žaloby o neplatnosť sa zákonnosť aktu musí posudzovať v závislosti od skutkových a právnych okolností existujúcich v čase, keď bol akt prijatý, pričom posúdenie Komisie možno spochybniť len v prípade, ak sa javí byť zjavne nesprávne vzhľadom na informácie, ktoré Komisia mala k dispozícii v čase prijatia predmetného aktu“ [52].

132. Súdny dvor vo svojom rozsudku Gaz de France – Berliner Investissement [53] pripomenul zásadu, že „posúdenie platnosti aktu, ktoré prináleží vykonať Súdnemu dvoru v rámci prejudiciálneho konania, sa má za normálnych okolností oprieť o situáciu, ktorá existovala v čase prijatia aktu“ [54]. Podľa všetkého však uznal, že „platnosť aktu [by] bolo možné v niektorých prípadoch posúdiť podľa nových skutočností, ktoré vzišli najavo až po jeho prijatí“ [55].

133. Tento otvorenejší prístup, ktorý takto načrtol Súdny dvor, považujem za mimoriadne relevantný v rámci prejednávanej veci.

134. Rozhodnutia prijaté Komisiou na základe článku 25 ods. 6 smernice 95/46 majú totiž špecifické znaky. Ich cieľom je posúdiť, či úroveň ochrany osobných údajov, ktorú poskytuje tretia krajina, je alebo nie je primeraná. Ide tu o posúdenie, ktoré sa nevyhnutne mení v závislosti od skutkových a právnych okolností v tretej krajine.

135. Vzhľadom na to, že rozhodnutie o primeranosti je osobitným typom rozhodnutia, pravidlo, že jeho platnosť možno posudzovať len v závislosti od okolností, ktoré existovali v čase jeho prijatia, treba v prejednávanom prípade upraviť. V opačnom prípade by také pravidlo viedlo k tomu, že niekoľko rokov po prijatí rozhodnutia o primeranosti by sa pri posudzovaní platnosti, ktoré má vykonať Súdny dvor, nemohli zohľadniť udalosti, ku ktorým došlo neskôr, a to aj napriek tomu, že návrh na začatie prejudiciálneho konania týkajúci sa posúdenia platnosti nie je časovo obmedzený a jeho podanie môže byť práve dôsledkom neskorších skutočností, ktoré svedčia o nedostatkoch predmetného aktu.

52 — Pozri najmä rozsudok BVGD/Komisia (T-104/07 a T-339/08, EU:T:2013:366, bod 291), ktorý odkazuje na rozsudok IECC/Komisia (C-449/98 P, EU:C:2001:275, bod 87).

53 — C-247/08, EU:C:2009:600.

54 — Bod 49 a citovaná judikatúra.

55 — Bod 50 a citovaná judikatúra. Pozri v tomto zmysle LENAERTS, K., MASELIS, I., GUTMAN, K.: *EU Procedural Law*. Oxford University Press, 2014, ktorí uvádzajú, že, „in certain cases, the validity of the particular Union measure can be assessed by reference to new factors arising after that measure was adopted, depending on the determination of the Court“ (bod 10.16, s. 471).

136. Skutočnosť, že rozhodnutie 2000/520 platí približne pätnásť rokov, v prejednávanom prípade svedčí o konkludentnom súhlase Komisie s jej posúdením vykonaným v roku 2000. Ak má Súdny dvor v prejudiciálnom konaní zhodnotiť platnosť posúdenia, na ktorom Komisia stále trvá, je nielen možné, ale aj vhodné, aby mohol porovnať toto posúdenie s novými okolnosťami, ktoré nastali od prijatia rozhodnutia o primeranosti.

137. Vzhľadom na osobitnú povahu rozhodnutia o primeranosti Komisia musí toto rozhodnutie pravidelne preskúmavať. Ak Komisia v dôsledku nových udalostí, ku ktorým medzičasom došlo, nezmení svoje rozhodnutie, konkludentne, ale nevyhnutne potvrdí svoje pôvodné posúdenie. Opakuje tak svoje konštatovanie, že príslušná tretia krajina zabezpečuje primeranú úroveň ochrany prenášaných osobných údajov. Je úlohou Súdneho dvora preskúmať, či je toto konštatovanie napriek okolnostiam, ktoré nastali neskôr, naďalej pravdivé.

138. S cieľom zabezpečiť účinné súdne preskúmanie rozhodnutia tohto typu teda podľa môjho názoru treba posúdiť platnosť tohto rozhodnutia s prihliadnutím na súčasný skutkový a právny rámec.

2. O pojme primeraná úroveň ochrany

139. Článok 25 smernice 95/46 úplne spočíva na zásade, že k prenosu osobných údajov do tretej krajiny môže dôjsť len vtedy, ak táto tretia krajina zaistí primeranú úroveň ochrany takých údajov. Cieľom tohto článku je teda zaručiť nepretržitosť ochrany poskytovanej touto smernicou v prípade prenosu osobných údajov do tretej krajiny. V tejto súvislosti treba pripomenúť, že uvedená smernica poskytuje vysokú úroveň ochrany občanov Únie pri spracovaní ich osobných údajov.

140. Vzhľadom na dôležitú úlohu, ktorú ochrana osobných údajov zohráva s ohľadom na základné právo na rešpektovanie súkromia, musí byť zabezpečená taká vysoká úroveň ochrany, a to aj v prípade prenosu osobných údajov do tretej krajiny.

141. Preto sa domnievam, že Komisia môže na základe článku 25 ods. 6 smernice 95/46 konštatovať, že tretia krajina zaisťuje primeranú úroveň ochrany, len v prípade, ak je po celkovom posúdení práva a praxe predmetnej tretej krajiny schopná preukázať, že táto tretia krajina poskytuje úroveň ochrany, ktorá je v podstate rovnocenná úrovni ochrany poskytovanej touto smernicou, aj keď pravidlá poskytovania tejto ochrany môžu byť odlišné od pravidiel, ktoré bežne platia v rámci Únie.

142. Hoci anglický výraz „adequate“ možno z jazykového hľadiska chápať tak, že označuje úroveň ochrany, ktorá je len uspokojivá alebo dostatočná, a teda môže mať iný sémantický rozsah ako francúzsky výraz „adéquat“, je potrebné poznamenať, že jediným kritériom, ktorým sa treba riadiť pri výklade tohto výrazu, je cieľ spočívajúci v dosiahnutí vysokej úrovne ochrany základných práv, ako to vyžaduje smernica 95/46.

143. Skúmanie úrovne ochrany poskytovanej treťou krajinou musí byť zamerané na dve základné okolnosti, ktorými sú obsah uplatniteľných pravidiel a prostriedky na zabezpečenie dodržiavania týchto pravidiel. [56]

144. Aby sa dosiahla úroveň ochrany, ktorá je v podstate rovnocenná úrovni ochrany platnej v rámci Únie, podľa môjho názoru by mali byť s režimom bezpečného prístavu, ktorý spočíva do veľkej miery na samocertifikácii a samoposúdení podnikmi, ktoré sa dobrovoľne zúčastňujú na tomto režime, spojené primerané záruky a dostatočný kontrolný mechanizmus. Prenosy osobných údajov do tretích krajín by teda nemali byť chránené v menšej miere ako spracovanie osobných údajov v rámci Únie.

56 — Pozri s. 5 pracovného dokumentu WP 12 Komisie s názvom „Prenosy osobných údajov do tretích krajín: Uplatňovanie článkov 25 a 26 smernice o ochrane údajov“, ktorý prijala Pracovná skupina pre ochranu jednotlivcov so zreteľom na spracovanie osobných údajov 24. júla 1998.

145. V tejto súvislosti hneď na úvod poznamenávam, že v rámci Únie prevláda názor, že mechanizmus externej kontroly v podobe nezávislého orgánu tvorí nevyhnutnú súčasť každého systému, ktorého cieľom je zabezpečiť dodržiavanie pravidiel týkajúcich sa ochrany osobných údajov.

146. Okrem toho s cieľom zabezpečiť potrebný účinok článku 25 ods. 1 a 3 smernice 95/46 treba vziať do úvahy skutočnosť, že primeranosť úrovne ochrany poskytovanej treťou krajinou je vyvíjajúcim sa stavom, ktorý sa môže postupom času meniť v závislosti od viacerých faktorov. Členské štáty a Komisia musia preto sústavne venovať pozornosť akejkoľvek zmene okolností, ktorá by si mohla vyžadovať prehodnotenie primeranosti úrovne ochrany poskytovanej treťou krajinou. Hodnotenie primeranosti tejto úrovne ochrany vôbec nemožno obmedziť na konkrétny okamih a potom ho ponechať v platnosti bez časového obmedzenia, nezávisle od akejkoľvek zmeny okolností, ktorá svedčí o tom, že úroveň poskytovanej ochrany v skutočnosti už nie je primeraná.

147. Povinnosť tretej krajiny zabezpečiť primeranú úroveň ochrany je teda trvalou povinnosťou. Ak sa hodnotenie vykoná v určitom okamihu, rozhodnutie o primeranosti možno ponechať v platnosti len za predpokladu, že odvtedy nenastala nijaká okolnosť, ktorá by mohla spochybniť pôvodné hodnotenie Komisie.

148. Netreba totiž zabúdať na to, že cieľom článku 25 smernice 95/46 je zabrániť prenosu osobných údajov do tretej krajiny, ktorá nezabezpečuje primeranú úroveň ochrany, v rozpore so základným právom na ochranu osobných údajov zaručeným v článku 8 Charty.

149. Je potrebné zdôrazniť, že právomoc konštatovať, že tretia krajina zaisťuje primeranú úroveň ochrany, ktorú normotvorca Únie priznáva Komisii v článku 25 ods. 6 smernice 95/46, je výslovne podriadená požiadavke, aby táto tretia krajina zaisťovala takú úroveň v zmysle odseku 2 tohto článku. Ak nové okolnosti spochybňujú jej pôvodné hodnotenie, Komisia by mala v dôsledku toho upraviť svoje rozhodnutie.

3. Moje posúdenie

150. Pripomínam, že podľa článku 25 ods. 6 smernice 95/46 „Komisia môže zistiť [konštatovať – *neoficiálny preklad*], podľa postupu uvedeného v článku 31 ods. 2, že tretia krajina zaisťuje adekvátnu úroveň ochrany v rámci znenia odseku 2 tohto článku, z dôvodu jej vnútroštátneho práva alebo medzinárodných dohôd, ktoré podpísala, najmä na základe záverov jednaní uvedených v odseku 5, na ochranu súkromného života a osobných práv a slobôd [slobôd a základných práv osôb – *neoficiálny preklad*]“. Článok 25 ods. 6 v spojení s článkom 25 ods. 2 tejto smernice znamená, že na účely konštatovania, že tretia krajina zaisťuje primeranú úroveň ochrany, musí Komisia vyhodnotiť všetky právne predpisy platné v tejto tretej krajine, ako aj ich uplatňovanie.

151. Ako už bolo uvedené, skutočnosť, že Komisia ponechala svoje rozhodnutie 2000/520 v platnosti napriek tomu, že nastali nové skutkové a právne okolnosti, treba chápať tak, že chcela potvrdiť svoje pôvodné hodnotenie.

152. Súdnemu dvoru v prejudiciálnom konaní neprináleží posudzovať skutkové okolnosti sporu, ktoré viedli vnútroštátny súd k podaniu návrhu na začatie prejudiciálneho konania. [57]

153. Budem teda vychádzať zo skutočností, ktoré uviedol vnútroštátny súd vo svojom návrhu na začatie prejudiciálneho konania, pričom samotná Komisia navyše do veľkej miery uznáva tieto skutočnosti za preukázané. [58]

57 — Pozri najmä rozsudok Fallimento Traghetti del Mediterraneo (C-140/09, EU:C:2010:335, bod 22 a citovanú judikatúru).

58 — Pozri oznámenie Komisie spomenuté v poznámke pod čiarou 2 a oznámenie Komisie Európskemu parlamentu a Rade o fungovaní systému bezpečného prístavu z pohľadu občanov EÚ a spoločností usadených v EÚ [COM(2013) 847 final].

154. Okolnosti, ktoré boli uvedené v konaní na Súdnom dvore s cieľom spochybniť posúdenie Komisie, podľa ktorého režim týkajúci sa bezpečného prístavu zaisťuje primeranú úroveň ochrany osobných údajov prenášaných z Únie do Spojených štátov, možno opísať takto.

155. Vnútroštátny súd vo svojom návrhu na začatie prejudiciálneho konania vychádza z týchto dvoch skutkových zistení. Po prvé osobné údaje, ktoré prenášajú podniky, ako napríklad Facebook Ireland, svojej materskej spoločnosti so sídlom v Spojených štátoch, sú potom dostupné pre NSA, ako aj pre iné bezpečnostné agentúry Spojených štátov v rámci masového a nediferencovaného sledovania a zaznamenávania takých údajov. V dôsledku zistení pána Snowdena totiž z dostupných dôkazov nemožno vyvodiť žiadny iný opodstatnený záver.[59] Po druhé občania Únie nemajú nijaké skutočné právo byť vypočutí v otázke sledovania a zaznamenávania ich údajov zo strany NSA alebo iných bezpečnostných agentúr Spojených štátov.[60]

156. Tieto skutkové zistenia, ku ktorým dospel High Court, sú podložené zisteniami, ku ktorým dospela samotná Komisia.

157. Komisia vo svojom vyššie uvedenom oznámení o fungovaní systému bezpečného prístavu z pohľadu občanov EÚ a spoločností usadených v EÚ vychádzala zo zistenia, že počas roka 2013 informácie o veľkosti a rozsahu programov sledovania USA vyvolali obavy o kontinuitu ochrany osobných údajov zákonne prenesených do USA podľa systému bezpečného prístavu. Poukázala na to, že všetky spoločnosti, ktoré sa zúčastňujú programu PRISM a umožňujú orgánom USA prístup k údajom uloženým a spracúvaným v USA, majú certifikát pre systém bezpečného prístavu. Podľa názoru Komisie sa tým systém bezpečného prístavu stal jedným z kanálov, cez ktorý majú spravodajské orgány USA prístup k zhromažďovaniu osobných údajov pôvodne spracovaných v EÚ.[61]

158. Z týchto skutočností vyplýva, že právo a prax Spojených štátov dovoľujú vo veľkom rozsahu zhromažďovať osobné údaje občanov Únie, ktoré sa prenášajú v rámci režimu bezpečného prístavu, bez toho, aby mali títo občania zaručenú účinnú súdnu ochranu.

159. Tieto skutkové zistenia podľa môjho názoru preukazujú, že rozhodnutie 2000/520 neobsahuje dostatok záruk. Vzhľadom na tento nedostatok záruk bolo toto rozhodnutie vykonané spôsobom, ktorý nezodpovedá požiadavkám stanoveným Chartou, ako aj smernicou 95/46.

160. Účelom rozhodnutia Komisie prijatého na základe článku 25 ods. 6 smernice 95/46 je konštatovať, že tretia krajina „zaisťuje“ primeranú úroveň ochrany. Výraz „zaisťuje“, ktorý je použitý v prítomnom čase, znamená, že predpokladom ponechania takého rozhodnutia v platnosti je, že toto rozhodnutie sa týka tretej krajiny, ktorá po jeho prijatí naďalej zaručuje primeranú úroveň ochrany.

161. Uvádzané zistenia týkajúce sa konania NSA, podľa ktorých NSA používa údaje prenesené v rámci režimu bezpečného prístavu, v skutočnosti poukázali na nedostatky právneho základu, ktorým je rozhodnutie 2000/520.

162. Nedostatky, na ktoré sa poukázalo počas tohto konania, sa nachádzajú konkrétnejšie v štvrtom odseku prílohy I tohto rozhodnutia.

59 — Bod 7 písm. c) rozhodnutia vnútroštátneho súdu.

60 — Bod 7 písm. b) rozhodnutia vnútroštátneho súdu.

61 — Strana 19 oznámenia Komisie.

163. Pripomínam, že podľa tohto ustanovenia „dodržiavanie… zásad [bezpečného prístavu] môže byť obmedzené: a) na mieru potrebnú na splnenie požiadaviek národnej bezpečnosti, verejného záujmu alebo vymáhania práva; b) zákonmi, nariadeniami vlády alebo precedenčným právom, ktoré ustanovujú protichodné povinnosti alebo výslovné oprávnenia, za predpokladu, že pri vykonávaní každého takéhoto oprávnenia môže organizácia preukázať, že jej nedodržiavanie zásad je obmedzené do tej miery, ktorá je potrebná na splnenie vyššie stojacich legitímnych záujmov vyplývajúcich z takéhoto oprávnenia“.

164. Problém vyplýva v podstate z toho, že orgány Spojených štátov využívajú výnimky stanovené v citovanom ustanovení. Vzhľadom na to, že tieto výnimky sú sformulované príliš všeobecne, ich vykonávanie zo strany týchto orgánov nie je obmedzené na to najnevyhnutnejšie.

165. Okrem tejto príliš všeobecnej formulácie treba poukázať aj na skutočnosť, že občania Únie nemajú primeraný prostriedok nápravy proti spracovaniu svojich osobných údajov na iné účely než tie, na ktoré boli tieto údaje pôvodne zhromaždené a potom prenesené do Spojených štátov.

166. Výnimky z uplatňovania zásad bezpečného prístavu stanovené v rozhodnutí 2000/520, najmä v súvislosti s požiadavkami národnej bezpečnosti, mali byť spojené so zavedením nezávislého kontrolného mechanizmu, ktorý by mohol zabrániť zistenému porušovaniu práva na súkromie.

167. Zistenia týkajúce sa praxe spravodajských služieb Spojených štátov, pokiaľ ide o všeobecné sledovanie údajov prenesených v režime bezpečného prístavu, teda poukázali na určité nedostatky špecifické pre rozhodnutie 2000/520.

168. Tvrdenia uvádzané v rámci prejednávanej veci nepreukazujú, že spoločnosť Facebook porušila zásady bezpečného prístavu. Ak certifikovaná spoločnosť, akou je Facebook USA, sprístupní orgánom Spojených štátov údaje, ktoré získala na základe prenosu z členského štátu, možno sa domnievať, že táto spoločnosť to robí s cieľom dodržať právne predpisy Spojených štátov. Vzhľadom na to, že rozhodnutie 2000/520 výslovne pripúšťa takú situáciu, lebo výnimky, ktoré sú v ňom uvedené, sú sformulované široko, v prejednávanej veci v skutočnosti ide o otázku zlučiteľnosti takých výnimiek s primárnym právom Únie.

169. V tomto smere treba zdôrazniť, že z ustálenej judikatúry Súdneho dvora vyplýva, že dodržiavanie ľudských práv predstavuje podmienku zákonnosti aktov Únie a že v Únii nemožno prijať opatrenia nezlučiteľné s ich dodržiavaním. [62]

170. Z judikatúry Súdneho dvora navyše vyplýva, že oznámenie zhromaždených osobných údajov tretím osobám, či už verejnoprávnym alebo súkromnoprávnym, predstavuje zásah do práva na rešpektovanie súkromia, „nech už je ich neskoršie použitie akékoľvek“ [63]. Súdny dvor navyše vo svojom rozsudku Digital Rights Ireland a i. [64] potvrdil, že povolenie prístupu príslušných vnútroštátnych orgánov k takým údajom predstavuje dodatočné porušenie tohto základného práva. [65] Okrem toho každá forma spracovania osobných údajov spadá pod článok 8 Charty a predstavuje zásah do práva na ochranu takých údajov. [66] Prístup spravodajských služieb Spojených štátov k prenášaným údajom teda tiež predstavuje zásah do základného práva na ochranu osobných údajov zaručeného článkom 8 Charty, keďže taký prístup je spracovaním týchto údajov.

62 — Pozri najmä rozsudok Kadi a Al Barakaat International Foundation/Rada a Komisia (C-402/05 P a C-415/05 P, EU:C:2008:461, bod 284, ako aj citovanú judikatúru).

63 — Rozsudok Österreichischer Rundfunk a i. (C-465/00, C-138/01 a C-139/01, EU:C:2003:294, bod 74).

64 — C-293/12 a C-594/12, EU:C:2014:238.

65 — Bod 35.

66 — Bod 36.

171. Ako Súdny dvor konštatoval v uvedenom rozsudku, takto vymedzený zásah je rozsiahly a treba ho považovať za zvlášť závažný vzhľadom na veľký počet dotknutých používateľov a množstvo prenášaných údajov. Tieto okolnosti spolu s tajnou povahou prístupu orgánov Spojených štátov k osobným údajom prenášaným do podnikov so sídlom v Spojených štátoch spôsobujú, že ide o mimoriadne závažný zásah.

172. Okrem toho občania Únie, ktorí sú používateľmi sociálnej siete Facebook, nie sú informovaní o tom, že ich osobné údaje budú všeobecne dostupné pre bezpečnostné agentúry Spojených štátov.

173. Tiež treba zdôrazniť, že vnútroštátny súd konštatoval, že občania Únie nemajú v Spojených štátoch nijaké skutočné právo byť vypočutí v otázke sledovania a zaznamenávania svojich údajov. FISC vykonáva dohľad, ale konanie na tomto súde je tajné a nekontradiktórne.[67] Domnievam sa, že tu ide o zásah do práva občanov Únie na účinný prostriedok nápravy chráneného článkom 47 Charty.

174. Je teda preukázaný zásah do základných práv chránených článkami 7, 8 a 47 Charty, ktorý dovoľujú výnimky zo zásad bezpečného prístavu uvedené v štvrtom odseku prílohy I rozhodnutia 2000/520.

175. Teraz treba overiť, či tento zásah je alebo nie je odôvodnený.

176. Podľa článku 52 ods. 1 Charty akékoľvek obmedzenie výkonu práv a slobôd uznaných v tejto charte musí byť ustanovené zákonom a rešpektovať podstatu týchto práv a slobôd. Za predpokladu dodržiavania zásady proporcionality možno tieto práva a slobody obmedziť len vtedy, ak je to nevyhnutné a skutočne to zodpovedá cieľom všeobecného záujmu, ktoré sú uznané Úniou, alebo ak je to potrebné na ochranu práv a slobôd iných.

177. Vzhľadom na takto vymedzené podmienky prípustnosti obmedzení výkonu práv a slobôd chránených Chartou silne pochybujem, či obmedzenia, o ktoré ide v prejednávanej veci, možno považovať za obmedzenia, ktoré rešpektujú podstatu článkov 7 a 8 Charty. Prístup spravodajských služieb Spojených štátov k prenášaným údajom sa totiž podľa všetkého vzťahuje na obsah elektronickej komunikácie, čo zasahuje do podstaty základného práva na rešpektovanie súkromia a ostatných práv zakotvených v článku 7 Charty. Okrem toho, keďže široká formulácia obmedzení stanovených v štvrtom odseku prílohy I rozhodnutia 2000/520 potenciálne umožňuje vylúčiť uplatnenie všetkých zásad bezpečného prístavu, možno sa domnievať, že tieto obmedzenia zasahujú do podstaty základného práva na ochranu osobných údajov.[68]

178. Čo sa týka otázky, či zistený zásah zodpovedá cieľu všeobecného záujmu, v prvom rade pripomínam, že podľa štvrtého odseku písm. b) prílohy I rozhodnutia 2000/520 môže byť dodržiavanie zásad bezpečného prístavu obmedzené „zákonmi, nariadeniami vlády alebo precedenčným právom, ktoré ustanovujú protichodné povinnosti alebo výslovné oprávnenia, za predpokladu, že pri vykonávaní každého takéhoto oprávnenia môže organizácia preukázať, že jej nedodržiavanie zásad je obmedzené do tej miery, ktorá je potrebná na splnenie vyššie stojacich legitímnych záujmov vyplývajúcich z takéhoto oprávnenia“.

179. Treba konštatovať, že „legitímne záujmy“, ktoré sú spomenuté v tomto ustanovení, nie sú vymedzené. Vyplýva z toho neistota, pokiaľ ide o – potenciálne mimoriadne široký – rozsah pôsobnosti tejto výnimky z uplatňovania zásad bezpečného prístavu podnikmi, ktoré sa zaviazali dodržiavať ich.

67 — Bod 7 písm. b) rozhodnutia vnútroštátneho súdu.

68 — Pozri v tejto súvislosti rozsudok Digital Rights Ireland a i. (C-293/12 a C-594/12, EU:C:2014:238, body 39 a 40).

180. Tento dojem potvrdzuje znenie vysvetliviek obsiahnutých v časti B prílohy IV rozhodnutia 2000/520 nazvanom „Explicitné zákonné oprávnenia“, a to najmä konštatovanie, že „je zrejmé, že tam, kde právo USA ukladá konfliktné povinnosti, organizácie v USA, či už sú účastníkmi systému bezpečného prístavu alebo nie, musia dodržiavať toto právo“. V súvislosti s explicitnými oprávneniami sa navyše uvádza, že „napriek tomu, že zásady bezpečného prístavu sú zamerané na preklenutie rozdielov medzi režimami ochrany súkromia v USA a v Európe, je potrebné sa podriadiť výsadným právomociam volených zákonodarcov“.

181. Z toho vyplýva, že táto výnimka je podľa môjho názoru v rozpore s článkami 7 a 8 a s článkom 52 ods. 1 Charty, keďže nesleduje dostatočne presne vymedzený cieľ všeobecného záujmu.

182. Jednoduchosť a všeobecnosť, s akými samotné rozhodnutie 2000/520 v štvrtom odseku písm. b) prílohy I a v časti B prílohy IV stanovuje, že zásady bezpečného prístavu možno vylúčiť na základe ustanovení práva Spojených štátov, sú v každom prípade nezlučiteľné s podmienkou, aby výnimky z pravidiel týkajúcich sa ochrany osobných údajov boli obmedzené na to najnevyhnutnejšie. Je tu síce spomenutá podmienka nevyhnutnosti, ale – odhliadnuc od toho, že za preukázanie splnenia tejto podmienky zodpovedá dotknutý podnik – mi nie je jasné, ako by sa taký podnik mohol zbaviť povinnosti neuplatniť zásady bezpečného prístavu, ktorá vyplýva z právnych predpisov, ktoré je povinný uplatňovať.

183. Preto zastávam názor, že rozhodnutie 2000/520 treba vyhlásiť za neplatné, keďže existencia výnimky, ktorá takým všeobecným a nepresným spôsobom umožňuje odchýliť sa od zásad režimu bezpečného prístavu, sama osebe bráni konštatovaniu, že tento režim zaisťuje primeranú úroveň ochrany osobných údajov, ktoré sa prenášajú z Únie do Spojených štátov.

184. Pokiaľ ide o prvú kategóriu obmedzení stanovených v štvrtom odseku písm. a) prílohy I rozhodnutia 2000/520 z dôvodu požiadaviek národnej bezpečnosti, verejného záujmu alebo vymáhania práva, domnievam sa, že len prvý cieľ je dostatočne presný na to, aby sa mohol považovať za cieľ všeobecného záujmu uznaný Úniou v zmysle článku 52 ods. 1 Charty.

185. Teraz treba overiť proporcionalitu zisteného zásahu.

186. V tejto súvislosti je potrebné pripomenúť, že „podľa ustálenej judikatúry Súdneho dvora zásada proporcionality vyžaduje, aby akty inštitúcií Únie boli vhodné na dosiahnutie legitímnych cieľov sledovaných predmetnou právnou úpravou a neprekračovali hranice toho, čo je primerané a potrebné na uskutočnenie týchto cieľov“ [69].

187. V súvislosti so súdnou kontrolou splnenia týchto podmienok, „keďže ide o zásahy do základných práv, môže byť rozsah voľnej úvahy normotvorcu Únie obmedzený na základe niekoľkých kritérií, ako sú predovšetkým dotknutá oblasť, povaha dotknutého práva zaručeného Chartou, povaha a závažnosť zásahu, ako aj jeho účel“ [70].

188. Domnievam sa, že rozhodnutia, ktoré Komisia prijme na základe článku 25 ods. 6 smernice 95/46, podliehajú úplnému preskúmaniu Súdneho dvora, pokiaľ ide o proporcionalitu posúdenia vykonaného touto inštitúciou v súvislosti s primeranosťou úrovne ochrany poskytovanej treťou krajinou z dôvodu „jej vnútroštátneho práva alebo medzinárodných dohôd, ktoré podpísala“.

69 — Rozsudok Digital Rights Ireland a i. (C-293/12 a C-594/12, EU:C:2014:238, bod 46, ako aj citovaná judikatúra).

70 — Tamže, bod 47 a citovaná judikatúra.

189. V tomto smere treba poznamenať, že Súdny dvor vo svojom rozsudku Digital Rights Ireland a i.[71] rozhodol, že „vzhľadom na dôležitú úlohu, ktorú na jednej strane zohráva ochrana osobných údajov so zreteľom na základné právo rešpektovania súkromného života, a na druhej strane, rozsah a závažnosť zásahu do tohto práva, ktorý obsahuje [predmetná] smernica…, je voľná úvaha normotvorcu Únie obmedzená, takže treba pristúpiť k prísnej kontrole“[72].

190. Taký zásah musí byť vhodný na dosiahnutie cieľa sledovaného predmetným aktom Únie a nevyhnutný na dosiahnutie tohto cieľa.

191. V tejto súvislosti, „pokiaľ ide o právo na rešpektovanie súkromného života, ochrana tohto základného práva podľa ustálenej judikatúry Súdneho dvora… vyžaduje, aby výnimky a obmedzenia v súvislosti s ochranou osobných údajov nepôsobili nad rámec toho, čo je prísne nevyhnutné“[73].

192. Súdny dvor pri svojom skúmaní berie do úvahy aj skutočnosť, že „ochrana osobných údajov, ktorá je výslovne stanovená v článku 8 ods. 1 Charty, má mimoriadny význam pre právo na rešpektovanie súkromného života zakotvené v jej článku 7“[74].

193. Podľa Súdneho dvora, ktorý v tejto súvislosti odkazuje na judikatúru Európskeho súdu pre ľudské práva, „musí dotknutá právna úprava Únie stanoviť jasné a presné pravidlá upravujúce rozsah a uplatnenie predmetného opatrenia a ukladajúce minimálne požiadavky spôsobom, aby osoby, ktorých údaje boli uchované, mali dostatočné záruky umožňujúce účinne chrániť ich osobné údaje proti rizikám zneužitia, ako aj proti akémukoľvek nezákonnému prístupu a akémukoľvek nezákonnému použitiu týchto údajov“[75]. Súdny dvor uvádza, že „nevyhnutnosť disponovať takými zárukami je o to dôležitejšia, keď sú osobné údaje… spracovávané automaticky a keď existuje značné riziko nezákonného prístupu k týmto údajom“[76].

194. Podľa môjho názoru existuje medzi štvrtým odsekom písm. a) prílohy I rozhodnutia 2000/520 a článkom 13 ods. 1 smernice 95/46 analogický vzťah. Prvé uvedené ustanovenie stanovuje, že dodržiavanie zásad bezpečného prístavu môže byť obmedzené „na mieru potrebnú na splnenie požiadaviek národnej bezpečnosti, verejného záujmu alebo vymáhania práva“. Podľa druhého uvedeného ustanovenia členské štáty môžu prijať legislatívne opatrenia na obmedzenie rozsahu povinností a práv uvedených v článku 6 ods. 1, v článku 10, v článku 11 ods. 1 a v článkoch 12 a 21 tejto smernice, keď takéto obmedzenie predstavuje nevyhnutné opatrenie okrem iného na ochranu štátnej bezpečnosti, obrany, verejnej bezpečnosti, ako aj na predchádzanie, vyšetrovanie, odhaľovanie a stíhanie trestných činov.

195. Ako Súdny dvor uviedol vo svojom rozsudku IPI[77], zo znenia článku 13 ods. 1 smernice 95/46 vyplýva, že členské štáty môžu prijať opatrenia uvedené v tomto ustanovení len vtedy, ak sú potrebné. „Nevyhnutný“ charakter týchto opatrení tak podmieňuje možnosť, ktorú toto ustanovenie poskytuje členským štátom.[78] Pokiaľ ide o spracovanie osobných údajov v rámci Únie, limity stanovené v článku 13 tejto smernice treba chápať tak, že sú obmedzené na to, čo je úplne nevyhnutné na dosiahnutie sledovaného cieľa. Domnievam sa, že to musí platiť aj v prípade obmedzení zásad bezpečného prístavu, ktoré sú stanovené v štvrtom odseku prílohy I rozhodnutia 2000/520.

71 — C-293/12 a C-594/12, EU:C:2014:238.

72 — Bod 48.

73 — Rozsudok Digital Rights Ireland a i. (C-293/12 a C-594/12, EU:C:2014:238, bod 52, ako aj citovaná judikatúra).

74 — Tamže, bod 53.

75 — Tamže, bod 54 a citovaná judikatúra.

76 — Tamže, bod 55 a citovaná judikatúra.

77 — C-473/12, EU:C:2013:715.

78 — Bod 32.

196. Treba pritom konštatovať, že kritérium nevyhnutnosti nie je spomenuté vo všetkých jazykových verziách štvrtého odseku písm. a) prílohy I rozhodnutia 2000/520. Tak je to okrem iného aj v prípade francúzskej verzie, v ktorej sa uvádza, že „[l]'adhésion aux principes peut être limitée par… les exigences relatives à la sécurité nationale, l'intérêt public et le respect des lois des États-Unis" („dodržiavanie zásad môže byť obmedzené… požiadavkami týkajúcimi sa národnej bezpečnosti, verejného záujmu a dodržiavania zákonov Spojených štátov"), zatiaľ čo napríklad v španielskej, nemeckej a anglickej verzii sa uvádza, že zavedené obmedzenia musia byť nevyhnutné na dosiahnutie uvedených cieľov.

197. Skutkové okolnosti, ktoré uvádza vnútroštátny súd a ktoré uviedla Komisia vo svojich vyššie uvedených oznámeniach, v každom prípade jasne ukazujú, že vykonávanie týchto obmedzení v praxi nie je obmedzené na to, čo je úplne nevyhnutné na dosiahnutie uvádzaných cieľov.

198. V tejto súvislosti poznamenávam, že prístup k prenášaným osobným údajom, ktorý majú spravodajské služby Spojených štátov, všeobecne zahŕňa akúkoľvek osobu a všetky spôsoby elektronickej komunikácie, ako aj všetky prenášané údaje, vrátane obsahu komunikácie, bez toho, aby existovalo akékoľvek rozlíšenie, obmedzenie alebo výnimka na základe sledovaného cieľa všeobecného záujmu. [79]

199. Prístup spravodajských služieb Spojených štátov k prenášaným údajom sa totiž všeobecným spôsobom týka všetkých osôb používajúcich elektronické komunikačné služby bez toho, aby dotknuté osoby museli predstavovať hrozbu pre národnú bezpečnosť. [80]

200. Také masívne a nediferencované sledovanie je samo osebe neprimerané a predstavuje neodôvodnený zásah do práv zaručených článkami 7 a 8 Charty.

201. Ako Parlament správne poznamenal vo svojich pripomienkach, keďže je vylúčené, aby normotvorca Únie alebo členské štáty prijali právne predpisy, ktoré by v rozpore s Chartou stanovovali masívne a nediferencované sledovanie, nevyhnutne z toho vyplýva, že *a fortiori* sa nemožno v nijakom prípade domnievať, že tretie krajiny zaisťujú primeranú úroveň ochrany osobných údajov občanov Únie, ak ich právna úprava skutočne povoľuje masívne a nediferencované sledovanie a zaznamenávanie tohto typu údajov.

202. Okrem toho treba zdôrazniť, že režim bezpečného prístavu, ako je vymedzený v rozhodnutí 2000/520, neobsahuje záruky, ktoré by mohli zabrániť masívnemu a všeobecnému sprístupneniu prenášaných údajov.

203. V tejto súvislosti poznamenávam, že Súdny dvor vo svojom rozsudku Digital Rights Ireland a i. [81] zdôraznil, že je dôležité stanoviť „jasné a presné pravidlá upravujúce rozsah zásahu do základných práv zakotvených v článkoch 7 a 8 Charty" [82]. Taký zásah musí byť podľa Súdneho dvora „presne vymedzený ustanoveniami, ktoré by mohli zaručiť, že sa tento zásah obmedzí iba na to najnevyhnutnejšie" [83]. Súdny dvor v tomto rozsudku tiež zdôraznil potrebu stanoviť „ dostatočné záruky, ako ich vyžaduje článok 8 Charty, ktoré umožňujú zabezpečiť účinnú ochranu [osobných] údajov pred rizikom zneužitia, ako aj pred akýmkoľvek nezákonným prístupom a každým nezákonným použitím týchto údajov" [84].

79 — Pozri analogicky rozsudok Digital Rights Ireland a i. (C-293/12 a C-594/12, EU:C:2014:238, bod 57 a citovanú judikatúru).

80 — Tamže, body 58 a 59.

81 — C-293/12 a C-594/12, EU:C:2014:238.

82 — Bod 65.

83 — Tamže.

84 — Tamže, bod 66.

204. Treba pritom konštatovať, že mechanizmy súkromnej arbitráže a FTC vzhľadom na to, že ich úloha je obmedzená na spory obchodnej povahy, nepredstavujú prostriedky na spochybnenie sprístupnenia osobných údajov prenášaných z Únie spravodajským službám Spojených štátov.

205. Právomoc FTC sa vzťahuje na nekalé alebo klamlivé konanie alebo postupy v rámci obchodovania, a teda sa nevzťahuje na zhromažďovanie a využívanie osobných informácií na nekomerčné účely. [85] Obmedzená pôsobnosť FTC obmedzuje právo jednotlivcov na ochranu ich osobných údajov. FTC nebol vytvorený s cieľom zabezpečiť – ako je to v prípade vnútroštátnych dozorných orgánov v rámci Únie – ochranu individuálneho práva na súkromie, ale s cieľom zaručiť poctivé a spoľahlivé obchodovanie pre spotrebiteľov, čo *de facto* obmedzuje možnosti zásahu FTC v oblasti týkajúcej sa ochrany osobných údajov. Úloha, ktorú zohráva FTC, teda nie je porovnateľná s úlohou vnútroštátnych dozorných orgánov upravených v článku 28 smernice 95/46.

206. Občania Únie, ktorých údaje boli prenesené, sa môžu obrátiť na špecializované arbitrážne orgány so sídlom v Spojených štátoch, ako napríklad TRUSTe a BBBOnline, so žiadosťou o informáciu, či podnik, ktorý uchováva ich osobné údaje, porušuje podmienky režimu samocertifikácie. Súkromná arbitráž, ktorú zabezpečujú subjekty ako TRUSTe, sa nemôže týkať porušení práva na ochranu osobných údajov, ktorých sa dopustia subjekty alebo orgány odlišné od samocertifikovaných podnikov. Tieto arbitrážne ustanovizne vôbec nemajú právomoc rozhodovať o zákonnosti činností bezpečnostných agentúr Spojených štátov.

207. FTC ani ustanovizne súkromnej arbitráže teda nemajú právomoc skúmať prípadné porušenia zásad ochrany osobných údajov, ktorých sa dopustili verejní aktéri, akými sú bezpečnostné agentúry Spojených štátov. Taká právomoc by však bola nevyhnutná na úplné zaručenie práva na účinnú ochranu týchto údajov. Komisia teda tým, že prijala rozhodnutie 2000/520 a ponechala ho v platnosti, nemohla konštatovať, že v prípade všetkých osobných údajov, ktoré budú prenesené do Spojených štátov, sa zabezpečí primeraná ochrana práva, ktoré zaručuje článok 8 ods. 3 Charty, teda že nezávislý orgán bude účinne dohliadať na dodržiavanie požiadaviek týkajúcich sa ochrany a bezpečnosti týchto údajov.

208. Preto treba konštatovať, že v rámci režimu bezpečného prístavu upraveného rozhodnutím 2000/520 chýba nezávislý orgán, ktorý by mohol dohliadať na to, aby vykonávanie výnimiek zo zásad bezpečného prístavu bolo obmedzené na to najnevyhnutnejšie. Ako pritom už bolo uvedené, taká kontrola vykonávaná nezávislým orgánom predstavuje z pohľadu práva Únie základný prvok ochrany osôb v súvislosti so spracovaním osobných údajov. [86]

209. V tejto súvislosti treba zdôrazniť úlohu, ktorú vnútroštátne dozorné orgány zohrávajú v systéme ochrany osobných údajov platnom v rámci Únie pri dohľade nad obmedzeniami stanovenými v článku 13 smernice 95/46. Podľa článku 28 ods. 4 druhého pododseku tejto smernice „každý dozorný orgán [posúdi] najmä nároky na kontrolu zákonnosti spracovania údajov, uplatnené každou osobou, keď sa uplatňujú vnútroštátne ustanovenia prijaté v súlade s článkom 13 tejto smernice“. Analogicky sa domnievam, že zmienka o obmedzeniach uplatňovania zásad bezpečného prístavu v štvrtom odseku prílohy I rozhodnutia 2000/520 mala byť spojená so zavedením kontrolného mechanizmu prevádzkovaného nezávislým orgánom špecializovaným na oblasť ochrany osobných údajov.

210. Zásah nezávislých dozorných orgánov totiž tvorí podstatu európskeho systému ochrany osobných údajov. Je teda prirodzené, že existencia takých orgánov sa už od začiatku považovala za jednu z nevyhnutných podmienok konštatovania primeranosti úrovne ochrany poskytovanej tretími krajinami. Splnenie tejto podmienky umožňuje, aby toky údajov z územia členských štátov na územie

85 — Pozri v tejto súvislosti prílohu II FAQ 11 rozhodnutia 2000/520 s názvom „Činnosť Federálnej obchodnej komisie (FTC – Federal Trade Commission)“ a prílohy III, V a VII tohto rozhodnutia.

86 — Pozri rozsudok Digital Rights Ireland a i. (C-293/12 a C-594/12, EU:C:2014:238, bod 68, ako aj citovanú judikatúru).

tretích krajín neboli zakázané podľa článku 25 smernice 95/46.[87] Ako sa uvádza v pracovnom dokumente, ktorý vypracovala pracovná skupina vytvorená na základe článku 29 tejto smernice, v Európe panuje široká zhoda v tom, že „mechanizmus ‚externej kontroly' v podobe nezávislého orgánu tvorí nevyhnutnú súčasť každého systému, ktorého cieľom je zabezpečiť dodržiavanie pravidiel týkajúcich sa ochrany údajov"[88].

211. Poukazujem navyše na to, že FISC neposkytuje občanom Únie, ktorých osobné údaje sa prenesú do Spojených štátov, účinný prostriedok nápravy. Ochrana pred sledovaním zo strany štátnych orgánov v zmysle článku 702 zákona o dohľade nad zahraničnými spravodajskými službami z roku 1978 sa totiž vzťahuje len na občanov Spojených štátov a na cudzích štátnych príslušníkov, ktorí sa legálne a trvalo zdržiavajú v Spojených štátoch. Ako poznamenala samotná Komisia, dohľad na programami spravodajských služieb USA na zhromažďovanie informácií by sa zlepšil posilnením úlohy FISC a zavedením nápravných opatrení pre jednotlivcov. Tieto mechanizmy by mohli obmedziť spracúvanie osobných údajov občanov Únie, ktoré nie sú potrebné na účely národnej bezpečnosti.[89]

212. Komisia navyše sama uviedla, že neexistujú žiadne príležitosti pre občanov Únie na získanie prístupu, opravu alebo vymazanie údajov, príležitosti na administratívnu alebo súdnu nápravu, pokiaľ ide o zhromažďovanie a ďalšie spracovanie ich osobných údajov, ku ktorému dochádza v rámci programov sledovania USA.[90]

213. Napokon treba spomenúť, že predpisy Spojených štátov týkajúce sa ochrany súkromia sa môžu uplatňovať na občanov Spojených štátov a cudzích štátnych príslušníkov odlišne.[91]

214. Z vyššie uvedeného vyplýva, že rozhodnutie 2000/520 nestanovuje jasné a presné pravidlá upravujúce rozsah zásahu do základných práv zakotvených v článkoch 7 a 8 Charty. Treba teda konštatovať, že toto rozhodnutie a uplatňovanie tohto rozhodnutia spôsobujú rozsiahly a mimoriadne závažný zásah do týchto základných práv, pričom taký zásah nie je presne vymedzený ustanoveniami, ktoré by mohli zaručiť, že sa obmedzí iba na to najnevyhnutnejšie.

215. Komisia teda tým, že prijala rozhodnutie 2000/520 a potom ho ponechala v platnosti, prekročila hranice, ktoré vyplývajú z rešpektovania zásady proporcionality s ohľadom na články 7 a 8 a článok 52 ods. 1 Charty. Navyše treba konštatovať, že došlo k neodôvodnenému zásahu do práva občanov Únie na účinný prostriedok nápravy zaručeného článkom 47 Charty.

216. Toto rozhodnutie treba preto vyhlásiť za neplatné, keďže z dôvodu porušení základných práv, ktoré boli opísané vyššie, sa nemožno domnievať, že režim bezpečného prístavu zavedený týmto rozhodnutím zaisťuje primeranú úroveň ochrany osobných údajov, ktoré sa v rámci tohto režimu prenášajú z Únie do Spojených štátov.

217. Vzhľadom na také konštatovanie porušení základných práv občanov Únie sa domnievam, že Komisia mala pozastaviť uplatňovanie rozhodnutia 2000/520.

218. Platnosť tohto rozhodnutia nie je časovo obmedzená. Prejednávaná vec pritom svedčí o tom, že primeranosť úrovne ochrany poskytovanej treťou krajinou sa môže postupom času meniť v závislosti od zmeny skutkových, ako aj právnych okolností, z ktorých uvedené rozhodnutie vychádza.

87 — Pozri POULLET, Y.: L'autorité de contrôle: „vues" de Bruxelles. In: *Revue française d'administration publique*, č. 89, január – marec 1999, s. 69, najmä s. 71.

88 — Pozri s. 7 pracovného dokumentu WP 12 Komisie spomenutého v poznámke pod čiarou 56.

89 — Strany 10 a 11 oznámenia Komisie spomenutého v poznámke pod čiarou 2.

90 — Pozri bod 7.2, s. 20, oznámenia Komisie spomenutého v poznámke pod čiarou 58.

91 — Pozri o tejto otázke KUNER, C.: Foreign Nationals and Data Protection Law: A Transatlantic Analysis. In: *Data Protection Anno 2014: How To Restore Trust*? Cambridge: Intersentia, 2014, s. 213, najmä s. 216 a nasl.

219. Poukazujem na to, že samotné rozhodnutie 2000/520 obsahuje ustanovenia, podľa ktorých môže Komisia v závislosti od okolností upraviť toto rozhodnutie.

220. Z odôvodnenia 9 tohto rozhodnutia vyplýva, že „‚bezpečný prístav' ustanovený zásadami a FAQ bude možno potrebné opätovne prehodnotiť na základe skúseností, na základe vývoja v oblasti ochrany súkromia za okolností, v ktorých technológia umožňuje čoraz jednoduchší prenos a spracúvanie osobných údajov a na základe správ o vykonávaní vypracovaných príslušnými orgánmi poverenými vymáhaním výkonu zásad a FAQ".

221. Článok 3 ods. 4 uvedeného rozhodnutia rovnako stanovuje, že „ak informácie zhromaždené podľa odsekov 1, 2 a 3 poskytujú dôkazy o tom, že určitý orgán zodpovedný za dodržiavanie zásad vykonávaných v súlade s FAQ v Spojených štátoch nevykonáva účinne svoju úlohu, Komisia o tom informuje Ministerstvo obchodu USA a v prípade potreby predloží návrh opatrení… s cieľom zrušiť alebo pozastaviť účinnosť tohto rozhodnutia alebo obmedziť rozsah jeho pôsobnosti".

222. Okrem toho podľa článku 4 ods. 1 rozhodnutia 2000/520 „toto rozhodnutie je možné kedykoľvek upraviť na základe skúseností s jeho vykonávaním a/alebo vtedy, ak úroveň ochrany poskytovanú zásadami a FAQ predstihnú požiadavky právnych predpisov USA. Komisia v každom prípade posúdi vykonávanie tohto rozhodnutia na základe dostupných informácií tri roky po jeho oznámení členským štátom a podá správu o príslušných zisteniach výboru ustanovenému podľa článku 31 smernice 95/46…, vrátane akýchkoľvek dôkazov, ktoré by mohli mať vplyv na hodnotenie, podľa ktorého ustanovenia uvedené v článku 1 tohto rozhodnutia poskytujú primeranú ochranu v zmysle článku 25 smernice 95/46". V zmysle článku 4 ods. 2 rozhodnutia 2000/520 „Komisia v prípade potreby predloží návrh opatrení v súlade s postupom uvedeným v článku 31 smernice 95/46".

223. Komisia vo svojich pripomienkach konštatovala, že je „veľmi pravdepodobné…, že dodržiavanie zásad bezpečného prístavu bolo obmedzené takým spôsobom, ktorý už nezodpovedá prísne vymedzeným podmienkam výnimky týkajúcej sa národnej bezpečnosti"[92]. Komisia v tomto smere poznamenáva, že „predmetné zistenia svedčia o masovom a nediferencovanom sledovaní, ktoré je nezlučiteľné s kritériom nevyhnutnosti stanoveným v tejto výnimke a vo všeobecnosti ani s právom na ochranu osobných údajov zakotveným v článku 8 Charty"[93]. Komisia navyše sama konštatovala, že „dosah programov sledovania v spojení s nerovným zaobchádzaním s občanmi [Únie] spochybňuje úroveň ochrany poskytovanej režimom bezpečného prístavu"[94].

224. Komisia na pojednávaní navyše výslovne uznala, že v rámci rozhodnutia 2000/520, ako sa uplatňuje v súčasnosti, neexistuje záruka, že právo občanov Únie na ochranu ich údajov bude zabezpečené. Toto konštatovanie však podľa jej názoru nemá vplyv na platnosť tohto rozhodnutia. Hoci Komisia súhlasí s tvrdením, že musí konať so zreteľom na nové okolnosti, domnieva sa, že prijala vhodné a primerané opatrenia tým, že začala rokovania so Spojenými štátmi s cieľom upraviť režim bezpečného prístavu.

225. Nestotožňujem sa s týmto názorom. Dovtedy totiž musí byť možné pozastaviť prenosy osobných údajov do Spojených štátov na podnet vnútroštátnych dozorných orgánov alebo na základe sťažností predložených týmto orgánom.

226. Okrem toho zastávam názor, že vzhľadom na také konštatovania mala Komisia pozastaviť uplatňovanie rozhodnutia 2000/520. Z cieľa týkajúceho sa ochrany osobných údajov, ktorý sleduje smernica 95/46, ako aj článok 8 Charty, totiž vyplývajú povinnosti nielen členským štátom, ale aj inštitúciám Únie, ako to vyplýva článku 51 ods. 1 Charty.

92 — Bod 44.

93 — Tamže.

94 — Pozri s. 5 oznámenia Komisie spomenutého v poznámke pod čiarou 2.

227. Komisia musí pri hodnotení úrovne ochrany poskytovanej treťou krajinou preskúmať nielen vnútroštátne predpisy a medzinárodné záväzky tejto tretej krajiny, ale aj spôsob, akým sa ochrana osobných údajov zabezpečuje v praxi. Ak z preskúmania praxe vyplynú nedostatky, Komisia musí reagovať a v prípade potreby bezodkladne pozastaviť a/alebo upraviť svoje rozhodnutie.

228. Ako som už uviedol vyššie, povinnosť, ktorú majú členské štáty, spočíva predovšetkým v tom, aby činnosťou svojich vnútroštátnych dozorných orgánov zabezpečili dodržiavanie pravidiel stanovených v smernici 95/46.

229. Povinnosťou Komisie je pozastaviť uplatňovanie rozhodnutia, ktoré prijala na základe článku 25 ods. 6 tejto smernice, v prípade preukázaných nedostatkov na strane príslušnej tretej krajiny, kým vedie rokovania s touto treťou krajinou s cieľom odstrániť tieto nedostatky.

230. Pripomínam, že účelom rozhodnutia Komisie prijatého na základe tohto ustanovenia je konštatovať, že tretia krajina „zaisťuje“ primeranú úroveň ochrany osobných údajov, ktoré sa prenášajú do tejto tretej krajiny. Výraz „zaisťuje“, ktorý je použitý v prítomnom čase, znamená, že predpokladom ponechania takého rozhodnutia v platnosti je, že toto rozhodnutie sa týka tretej krajiny, ktorá po jeho prijatí naďalej zaručuje takú primeranú úroveň ochrany.

231. Podľa odôvodnenia 57 smernice 95/46 „transfer osobných údajov do tretej krajiny, ktorá nezaisťuje adekvátnu úroveň ochrany, sa musí zakázať“.

232. V článku 25 ods. 4 tejto smernice sa uvádza, že „ak Komisia zistí [konštatuje – *neoficiálny preklad*], podľa postupu uvedeného v článku 31 ods. 2, že tretia krajina nezaisťuje adekvátnu úroveň ochrany v rámci znenia odseku 2 tohto článku, členské štáty podniknú nevyhnutné opatrenia na ochranu a prenos [na zamedzenie akéhokoľvek prenosu – *neoficiálny preklad*] údajov tohto istého typu do príslušnej tretej krajiny“. Článok 25 ods. 5 uvedenej smernice navyše stanovuje, že „vo vhodnom čase Komisia začne vyjednávať s cieľom napravenia stavu vzniknutého z vykonaných zistení [stavu vyplývajúceho z konštatovania, ku ktorému dospela – *neoficiálny preklad*] v súlade s odsekom 4“.

233. Z tohto posledného uvedeného ustanovenia vyplýva, že v systéme vytvorenom článkom 25 smernice 95/46 je cieľom rokovaní začatých s treťou krajinou napraviť neexistenciu primeranej úrovne ochrany konštatovanú podľa postupu uvedeného v článku 31 ods. 2 tejto smernice. V prejednávanom prípade Komisia podľa tohto postupu formálne nekonštatovala, že režim bezpečného prístavu už nezaisťuje primeranú úroveň ochrany. Ak sa však Komisia rozhodla začať rokovania so Spojenými štátmi, urobila to preto, lebo predtým usúdila, že úroveň ochrany, ktorú zaisťuje táto tretia krajina, už nie je primeraná.

234. Hoci Komisia vedela o nedostatkoch pri uplatňovaní rozhodnutia 2000/520, nepozastavila účinnosť tohto rozhodnutia ani ho neupravila, čím spôsobila pokračovanie porušovania základných práv osôb, ktorých osobné údaje boli prenesené a naďalej sa prenášajú v rámci režimu bezpečného prístavu.

235. Súdny dvor pritom už rozhodol – aj keď v inom kontexte –, že je úlohou Komisie zabezpečiť prijatie právnej úpravy vychádzajúcej z nových poznatkov. [95]

95 — Pozri v tomto zmysle rozsudok Agrarproduktion Staebelow (C-504/04, EU:C:2006:30, bod 40).

236. Také opomenutie Komisie, ktoré priamo porušuje základné práva zaručené článkami 7, 8 a 47 Charty, je podľa môjho názoru ďalším dôvodom na to, aby bolo rozhodnutie 2000/520 v tomto prejudiciálnom konaní vyhlásené za neplatné. [96]

III – **Návrh**

237. Vzhľadom na vyššie uvedené úvahy navrhujem, aby Súdny dvor odpovedal na otázky, ktoré položil High Court, takto:

Článok 28 smernice Európskeho parlamentu a Rady 95/46/ES z 24. októbra 1995 o ochrane fyzických osôb pri spracovaní osobných údajov a voľnom pohybe týchto údajov v spojení s článkami 7 a 8 Charty základných práv Európskej únie sa má vykladať v tom zmysle, že existencia rozhodnutia Európskej komisie prijatého na základe článku 25 ods. 6 smernice 95/46 nebráni vnútroštátnemu dozornému orgánu v tom, aby prešetril sťažnosť, v ktorej sa uvádza, že tretia krajina nezabezpečuje primeranú úroveň ochrany prenášaných osobných údajov, a prípadne pozastavil prenos týchto údajov.

Rozhodnutie Komisie 2000/520/ES z 26. júla 2000 v súlade so smernicou Európskeho parlamentu a Rady 95/46/ES o primeranosti ochrany poskytovanej zásadami „bezpečného prístavu“ a súvisiacimi často kladenými otázkami vydanými Ministerstvom obchodu USA je neplatné.

96 — Hoci Súdny dvor vo svojom rozsudku T. Port (C-68/95, EU:C:1996:452) rozhodol, že „Zmluva neumožňuje podať návrh na začatie prejudiciálneho konania, ktorým by vnútroštátny súd navrhol, aby Súdny dvor v prejudiciálnom konaní konštatoval nečinnosť inštitúcie“ (bod 53), zdá sa, že vo svojom rozsudku Ten Kate Holding Musselkanaal a i. (C-511/03, EU:C:2005:625, bod 29) zaujal k tejto možnosti priaznivejší postoj.