Sbírka soudních rozhodnutí

STANOVISKO GENERÁLNÍHO ADVOKÁTA
YVESE BOTA
přednesené dne 23. září 2015 [1]

**Věc C-362/14**

**Maximillian Schrems**
**proti**
**Data Protection Commissioner**

[žádost o rozhodnutí o předběžné otázce podaná High Court (Vrchní soud, Irsko)]

„Řízení o předběžné otázce — Osobní údaje — Ochrana fyzických osob v souvislosti se zpracováním těchto údajů — Listina základních práv Evropské unie — Články 7, 8 a 47 — Směrnice 95/46/ES — Článek 25 — Rozhodnutí 2000/520/ES — Předávání osobních údajů do Spojených států — Posouzení odpovídající, či neodpovídající úrovně ochrany — Stížnost fyzické osoby, jejíž osobní údaje byly předány do třetí země — Vnitrostátní orgán dozoru — Pravomoci“

## I – Úvod

1. Jak Evropská komise konstatovala ve sdělení ze dne 27. listopadu 2013 [2], „[p]ředávání osobních údajů je důležitým a nezbytným prvkem transatlantických vztahů. Tvoří nedílnou součást transatlantických obchodních výměn, mimo jiné pro potřeby nových rostoucích digitálních odvětví, jakými jsou sociální média nebo cloud computing, v jejichž rámci putuje z EU do USA velké množství údajů“ [3].

2. Obchodní výměny jsou předmětem rozhodnutí Komise 2000/520/ES ze dne 26. července 2000 podle směrnice Evropského parlamentu a Rady 95/46/ES o odpovídající ochraně poskytované podle zásad „bezpečného přístavu“, a s tím souvisejících „často kladených otázek“ vydaných ministerstvem obchodu Spojených států [4]. Toto rozhodnutí poskytuje právní základ pro předávání osobních údajů z Unie společnostem usazeným ve Spojených státech, které přijaly zásady „bezpečného přístavu“.

3. Uvedené rozhodnutí dnes čelí výzvě, jež spočívá v umožnění toků údajů z Unie do Spojených států a zároveň v zajištění vysoké úrovně ochrany těchto údajů, jak vyžaduje unijní právo.

4. Několik zjištění totiž v nedávné době odhalilo existenci amerických programů pro rozsáhlé shromažďování osobních údajů. Tato zjištění vyvolala pochybnosti o dodržování unijních právních norem při předávání osobních údajů společnostem usazeným ve Spojených státech a poukázala na slabiny režimu „bezpečného přístavu“.

1 — Původní jazyk: francouzština.

2 — Sdělení Komise Evropskému parlamentu a Radě, nazvané „Obnovení důvěry v toky údajů mezi EU a USA“ [COM(2013) 846 final].

3 — Strana 2.

4 — Úř. věst L 215, s. 7, a oprava Úř. věst. 2001, L 115, s. 14; Zvl. vyd. 16/01, s. 119.

5. Projednávaná žádost o rozhodnutí o předběžné otázce vyzývá Soudní dvůr k upřesnění, jaký přístup musí vnitrostátní orgány dozoru a Komise zaujmout v případě nesprávného uplatňování rozhodnutí 2000/520.

6. Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů [5] stanoví v kapitole IV pravidla pro předávání osobních údajů do třetích zemí.

7. V rámci této kapitoly je v čl. 25 odst. 1 této směrnice zakotvena zásada, podle které k předávání osobních údajů, které jsou předmětem zpracování nebo které mají být předmětem zpracování po předání, do třetích zemí může dojít, pouze pokud dotyčná třetí země zajistí odpovídající úroveň ochrany.

8. Jak uvádí bod 57 odůvodnění uvedené směrnice, v případě, kdy třetí země naopak neposkytuje odpovídající úroveň ochrany, musí být předávání osobních údajů do této země zakázáno.

9. Podle čl. 25 odst. 2 směrnice 95/46 „[o]dpovídající úroveň ochrany poskytovaná třetí zemí se posoudí s ohledem na všechny okolnosti související s předáním nebo předáváním údajů; zejména se přihlédne k povaze údajů, účelu a trvání předpokládaného či předpokládaných zpracování, zemi původu a zemi konečného určení, právním předpisům, obecným nebo zvláštním, platným v dotčené třetí zemi, jakož i profesním pravidlům a bezpečnostním opatřením, která jsou ve třetí zemi dodržována“.

10. Podle čl. 25 odst. 6 této směrnice může Komise konstatovat, že třetí země zajišťuje odpovídající úroveň ochrany osobních údajů na základě svých vnitrostátních předpisů nebo mezinárodních závazků. Jakmile Komise přijme rozhodnutí v tomto směru, k předání osobních údajů do dotyčné třetí země může dojít.

11. K provedení tohoto ustanovení přijala Komise rozhodnutí 2000/520. Z článku 1 odst. 1 tohoto rozhodnutí vyplývá, že „zásady ‚bezpečného přístavu‘“ prováděné podle pokynů obsažených v často kladených otázkách [6], zajišťují odpovídající úroveň ochrany osobních údajů předávaných z Unie společnostem usazeným ve Spojených státech.

12. V důsledku toho dovoluje rozhodnutí 2000/520 předávání osobních údajů z členských států společnostem usazeným ve Spojených státech, které se zavázaly k dodržování zásad „bezpečného přístavu“.

13. Rozhodnutí 2000/520 stanoví v příloze I několik zásad, k jejichž dodržování se mohou společnosti dobrovolně zavázat, společně s určitými omezeními a zvláštním systémem kontroly. Společností, které se zavázaly k dodržování tohoto tzv. „kodexu chování“, bylo v roce 2013 více než 3 200.

14. Režim „bezpečného přístavu“ spočívá na řešení, v němž se směšuje vlastní osvědčení a vlastní posouzení ze strany soukromých společností se zásahem veřejné moci.

15. Zásady „bezpečného přístavu“ byly vyvinuty „na základě konzultací s představiteli průmyslu a široké veřejnosti za účelem usnadnění obchodu mezi Spojenými státy a [Unií]. Jsou určeny výlučně organizacím ve Spojených státech, které získávají osobní údaje z [Unie], aby mohly splnit požadavky ‚bezpečného přístavu‘ a z něj vyplývající domněnku ‚odpovídající‘ ochrany údajů [7].

5 — Úř. věst. L 281, s. 31. Směrnice ve znění nařízení Evropského parlamentu a Rasy (ES) č. 1882/2003 ze dne 29. září 2003 (Úř. věst. L 284, s. 1; Zvl. vyd. 13/15, s. 355, dále jen „směrnice 95/46“).

6 — Frequently asked questions, dále jen „FAQ“.

7 — Druhý pododstavec přílohy I rozhodnutí 2000/520.

16. Zásady „bezpečného přístavu“ obsažené v příloze I rozhodnutí 2000/520 stanoví zejména:

— oznamovací povinnost, podle které „[o]rganizace musí informovat fyzické osoby o tom, za jakým účelem informace o nich shromažďuje a využívá, jak se mohou na organizaci obrátit v případě jakýchkoli dotazů nebo stížností, jakým třetím osobám tyto informace předává a jaké možnosti volby a prostředky tato organizace poskytuje fyzickým osobám, aby mohly omezit používání a předávání těchto informací. Toto oznámení musí být učiněno jasně a zřetelně při první příležitosti, při které je fyzická osoba požádána, aby poskytla organizaci své osobní údaje, nebo co možná nejdříve poté, avšak v každém případě před tím, než tato organizace takové údaje použije pro účely jiné, než pro jaké je předávající organizace původně shromáždila či zpracovala, nebo než je poprvé předá třetí osobě [8];

— povinnost organizací dát fyzickým osobám možnost zvolit, zda jejich osobní údaje mohou být předány třetí osobě nebo použity k účelu, který je neslučitelný s účelem (účely), ke kterému (kterým) byly původně shromážděny nebo následně dotčenou fyzickou osobou schváleny. U citlivých informací „musí být poskytnuta možnost potvrzující nebo výslovné volby (svolení), jestliže mají být tyto informace předány třetí osobě nebo použity k účelu, který neodpovídá účelu, pro který byly původně shromážděny nebo pro který byly následně dotčenou fyzickou osobou schváleny výkonem práva na volbu“ [9];

— pravidla pro další předání údajů. „Při předávání informací třetí osobě musí organizace uplatňovat zásady oznamovací povinnosti a možnosti volby [10];

— v souvislosti s bezpečností údajů povinnost pro „[o]rganizace, které vytvářejí, uchovávají, používají nebo šíří osobní údaje, […] učinit přiměřená bezpečnostní opatření, aby zabránily jejich ztrátě, zneužití a neoprávněnému přístupu k nim, jejich předávání, změně nebo zničení“ [11];

— v souvislosti s integritou údajů povinnost organizací „podniknout přiměřené kroky, aby zajistil[y] spolehlivost údajů pro zamýšlený účel, jejich přesnost, úplnost a aktuálnost [12];

— povinnost, že fyzické osoby, o nichž organizace uchovávají údaje, musí v zásadě „mít přístup k osobním údajům a musí mít možnost opravit, změnit nebo vymazat ty, které jsou nepřesné“ [13];

— povinnost zavést „mechanismy zajišťující dodržování zásad ‚bezpečného přístavu‘, opravné prostředky pro fyzické osoby, jichž se údaje týkají a které byly dotčeny nedodržením těchto zásad, jakož i sankce pro organizace, jestliže se zásadami neřídí“ [14].

17. Organizace Spojených států, které si přejí přijmout zásady „bezpečného přístavu“, musí v opatřeních na ochranu soukromí uvést, že veřejně přijímají tyto zásady a budou je dodržovat a samy se osvědčují tím, že ministerstvu obchodu Spojených států prohlásí, že dodržují uvedené zásady [15].

8 — Viz příloha I, pod nadpisem „Oznamovací povinnost“.

9 — Viz příloha I, pod nadpisem „Možnost volby“.

10 — Viz příloha I, pod nadpisem „Další předání“.

11 — Viz příloha I, pod nadpisem „Bezpečnost“.

12 — Viz příloha I, pod nadpisem „Integrita údajů“.

13 — Viz příloha I, pod nadpisem „Právo na přístup“.

14 — Viz příloha I, pod nadpisem „Prosazování“.

15 — Článek 1 odst. 2 a 3 rozhodnutí 2000/520. Viz též příloha II, FAQ 6.

18. Organizace disponují několika prostředky k dodržování zásad „bezpečného přístavu“. Mohou se například „připoj[it] k programu na ochranu soukromí, který byl vytvořen v soukromém sektoru a který je v souladu s těmito zásadami“ [nebo] tyto požadavky splnit také vytvořením vlastních opatření na ochranu soukromí, pokud jsou v souladu s těmito zásadami“. […] Dále mohou organizace podléhající právním a správním nebo jiným předpisům (nebo pravidlům), které účinně zajišťují ochranu osobních údajů, rovněž využívat výhod plynoucích z ‚bezpečného přístavu‘“ [16].

19. K ověřování, zda jsou dodržovány zásady „bezpečného přístavu“, existuje několik mechanismů směšujících soukromé rozhodčí řízení s dohledem orgánů veřejné moci. Dohled tedy může být zajišťován prostřednictvím systému mimosoudního řešení sporů nezávislým subjektem. Kromě toho se mohou společnosti zavázat ke spolupráci s orgánem Evropské unie pro ochranu údajů. Konečně k vyřizování stížností jsou příslušné Federální obchodní komise (Federal Trade Commission, dále jen „FTC“) na základě pravomocí, které jí byly svěřeny na základě oddílu 5 zákonu o Federální obchodní komisi (Federal Trade Commission Act), a ministerstvo dopravy (Department of Transportation) na základě pravomocí podle hlavy 49 United States Code oddíl 41712.

20. Podle čtvrtého pododstavce přílohy I rozhodnutí 2000/520 může být dodržování zásad „bezpečného přístavu“ omezeno zejména „v rozsahu nezbytném pro splnění požadavků bezpečnosti státu, veřejného zájmu nebo prosazování zákonů Spojených států“ nebo „zákonem, správním nařízením nebo judikaturou, které vytvářejí protichůdné závazky, nebo výslovným zmocněním za předpokladu, že při výkonu takového zmocnění může organizace prokázat, že nedodržení zásad je omezeno na rozsah nezbytný pro dodržení nadřazených oprávněných zájmů, jimž má takové zmocnění sloužit“ [17].

21. Kromě toho možnost příslušných orgánů členských států zastavit toky údajů podléhá několika podmínkám, jež jsou stanoveny v čl. 3 odst. 1 rozhodnutí 2000/520.

22. Projednávaná žádost o rozhodnutí o předběžné otázce vede k zamyšlení se nad dosahem rozhodnutí 2000/520, s ohledem na články 7, 8 a 47 Listiny základních práv Evropské unie (dále jen „Listina“), jakož i čl. 25 odst. 6 a článku 28 směrnice 95/46. Tato žádost byla předložena v rámci sporu mezi M. Schremsem a Data Protection Commissioner (komisař pro ochranu údajů, dále jen „Komisař“) ohledně odmítnutí Komisaře prošetřit stížnost podanou M. Schremsem z důvodu, že společnost Facebook Ireland Ltd (dále jen „Facebook Ireland“) uchovává osobní údaje o svých uživatelích na serverech umístěných ve Spojených státech.

23. Maximillian Schrems je rakouský státní příslušník s bydlištěm v Rakousku. Je uživatelem sociální sítě Facebook od roku 2008.

24. Od všech uživatelů Facebooku s bydlištěm na území Unie se vyžaduje, aby podepsali smlouvu se společností Facebook Ireland, která je dceřinou společností mateřské společnosti Facebook Inc., se sídlem ve Spojených státech (dále jen „Facebook USA“). Údaje o zákaznících společnosti Facebook Ireland s bydlištěm na území Unie jsou zcela nebo zčásti přenášeny na servery náležející společnosti Facebook USA umístěné na území Spojených států, kde jsou tyto údaje uchovávány.

25. M. Schrems podal dne 25. června 2013 ke Komisaři stížnost, v níž v podstatě tvrdil, že právní předpisy a praxe platné ve Spojených státech nezajišťují žádnou skutečnou ochranu údajů uchovávaných na území Spojených států před sledováním ze strany tohoto státu. To vyplývalo ze zjištění učiněných Edwardem Snowdenem od května 2013 ohledně činností amerických zpravodajských služeb, a konkrétně činností National Security Agency (dále jen „NSA“).

16 — Třetí pododstavec přílohy I.

17 — Viz též příloha IV část B.

26. Z těchto zjištění zejména vyplývá, že NSA vytvořila program nazvaný „PRISM“, v rámci něhož tato agentura získala volný přístup k hromadným údajům uloženým na serverech umístěných ve Spojených státech, které drží nebo nad nimiž dohlíží řada společností působících v oblasti internetu a technologií, jako je Facebook USA.

27. Komisař měl za to, že není povinen prošetřit stížnost, neboť ji považoval za po právní stránce nepodloženou. Shledal, že neexistují důkazy o tom, že by NSA skutečně využila možnosti přístupu k osobním údajům M. Schremse. Dále musela být stížnost podle něj zamítnuta z důvodu rozhodnutí 2000/520, v němž Komise konstatovala, že Spojené státy zajišťují v rámci režimu „bezpečného přístavu“ odpovídající úroveň ochrany předaných osobních údajů. Jakákoli otázka týkající se odpovídající ochrany osobních údajů ve Spojených státech musí být vyřešena v souladu s tímto rozhodnutím, které brání posouzení problému nadneseného v dané stížnosti.

28. Vnitrostátní předpisy, jež vedly Komisaře k zamítnutí stížnosti, jsou následující.

29. Článek 10 odst. 1 zákona z roku 1988 o ochraně osobních údajů (Data Protection Act 1988), ve znění zákona z roku 2003 o ochraně osobních údajů [Data Protection (Amendment) Act 2003, dále jen „zákon o ochraně osobních údajů“] svěřuje Komisaři pravomoc posoudit stížnosti a uvádí:

„a) Komisař může posoudit nebo nechat posoudit skutečnost, zda ustanovení tohoto zákona byla, jsou nebo by mohla být porušena ze strany dotyčné osoby, buď na základě stížnosti podané touto osobou pro porušení jakéhokoli tohoto ustanovení, nebo má-li Komisař za to, že k takovému porušení může dojít.

b) Podá-li dotyčná osoba stížnost ke Komisaři podle písmene a) tohoto odstavce, Komisař:

i) prošetří či nechá prošetřit stížnost, ledaže by dospěl k závěru, že stížnost je neopodstatněná nebo šikanózní, a

ii) nedojde-li v přiměřené lhůtě ke smírnému vyřízení stížnosti mezi dotyčnými stranami, oznámí písemně stěžovateli rozhodnutí, které přijme v souvislosti s danou stížností, přičemž uvede, že pokud toto rozhodnutí nepříznivě zasahuje do jeho právního postavení, může je stěžovatel napadnout soudní žalobou podle článku 26 tohoto zákona, ve lhůtě 21 dnů od doručení oznámení.“

30. V projednávané věci dospěl Komisař k závěru, že stížnost M. Schremse byla „neopodstatněná nebo šikanózní“ v tom smyslu, že byla odsouzena k neúspěchu, neboť nebyla po právní stránce podložená. Právě z tohoto důvodu odmítl Komisař tuto stížnost prošetřit.

31. Článek 11 zákona o ochraně osobních údajů upravuje předávání osobních údajů mimo území dotyčného státu. Článek 11 odst. 2 písm. a) tohoto zákona stanoví:

„Vyvstane-li v jakémkoli řízení, na které se vztahuje tento zákon, otázka:

i) za účelem určení, zda určitá země nebo území nacházející se mimo Evropský hospodářský prostor [(EHP)], do nichž mají být předány osobní údaje, zajišťuje odpovídající úroveň ochrany ve smyslu odstavce 1 tohoto článku a

ii) Unie učinila ve vztahu k předmětnému typu předání určité zjištění,

bude otázka vyřešena v souladu s tímto zjištěním.“

32. Článek 11 odst. 2 písm. b) zákona o ochraně osobních údajů definuje pojem „zjištění Unie“ následovně:

„V písmeně a) tohoto odstavce se ‚zjištěním Unie‘ rozumí zjištění, které Komise [...] učinila ve smyslu odstavců 4 nebo 6 článku 25 směrnice [95/46], v rámci postupu podle čl. 31 odst. 2 [této směrnice] s cílem určit, zda určitá země nebo území nacházející se mimo [EHP] zajišťují odpovídající úroveň ochrany uvedenou v odstavci 1 tohoto článku.“

33. Komisař poukázal na to, že rozhodnutí 2000/520 je „zjištěním Unie“ ve smyslu čl. 11 odst. 2 písm. a) zákona o ochraně osobních údajů, takže podle tohoto zákona musí být každá otázka týkající se odpovídající ochrany osobních údajů ve třetí zemi, do níž jsou tyto údaje předávány, vyřešena v souladu s tímto zjištěním. Vzhledem k tomu, že podstatou stížnosti žalobce bylo právě toto – tj. že osobní údaje byly předány do třetí země, která v praxi nezajišťuje odpovídající úroveň ochrany – měl Komisař za to, že povaha a samotná existence rozhodnutí 2000/520 mu brání v posouzení této otázky.

34. M. Schrems podal proti rozhodnutí Komisaře zamítajícímu jeho stížnost žalobu k High Court. Poté, co posoudil důkazy předložené v původním řízení, tento soud konstatoval, že elektronické sledování a zachycování osobních údajů států slouží nutným a nezbytným cílům, které jsou ve veřejném zájmu, a sice ochraně národní bezpečnosti a prevenci závažné trestné činnosti. High Court v této souvislosti uvedl, že sledování a zachycování osobních údajů předávaných z Unie do Spojených států slouží legitimním cílům souvisejícím s bojem proti terorismu.

35. Podle téhož soudu však zjištění učiněná E. Snowdenem prokázala, že se NSA a další podobné orgány dopustily značných přešlapů. Přestože existuje dohled ze strany Foreign Intelligence Surveillance Court (dále jen „FISC“), který působí v rámci zákona o sledování zahraničních zpravodajských služeb z roku 1978 (Foreign Intelligence Surveillance Act of 1978) [18], řízení před ním je tajné a nekontradiktorní. Navíc vedle toho, že rozhodnutí o přístupu k osobním údajům jsou přijímána na základě amerického práva, nemají unijní občané žádné účinné právo být vyslechnuti k otázce sledování a zachycování jejich údajů.

36. Z obsáhlých dokumentů přiložených k čestným prohlášením učiněným v původním řízení podle uvedeného soudu jasně vyplývá, že správnost četných zjištění učiněných E. Snowdenem není zpochybňována. High Court tudíž dospěl k závěru, že jakmile jsou osobní údaje předány do Spojených států, NSA a další americké bezpečnostní agentury, jako např. Federal Bureau of Investigation (FBI), mohou získat přístup k těmto údajům v rámci jimi prováděného rozsáhlého a nediferencovaného sledování a zachycování.

37. High Court konstatuje, že význam ústavních práv na respektování soukromého života a nedotknutelnosti obydlí v irském právu vyžaduje, aby jakýkoli zásah do těchto práv byl přiměřený a v souladu se zákonnými požadavky. Rozsáhlý a nediferencovaný přístup k osobním údajům nijak nesplňuje požadavek přiměřenosti, a musí být tudíž považován za v rozporu s irskou ústavou [19].

38. High Court podotýká, že k tomu, aby zachycování elektronických komunikací mohlo být považováno za slučitelné s touto ústavou, muselo by být prokázáno, že cílené zachycování komunikací a sledování určitých osob nebo skupin osob je objektivně odůvodněné v zájmu bezpečnosti státu nebo potírání trestné činnosti a že existují odpovídající a ověřitelné záruky.

18 — Viz oddíl 702 tohoto zákona, ve znění zákona z roku 2008 (Foreign Intelligence Surveillance Act of 2008). Právě na základě tohoto oddílu disponuje NSA databází známou pod názvem „PRISM“ (viz report on the Findings by the EU Co-chairs of the ad hoc EU-US Working Group on Data Protection ze dne 27. listopadu 2013).

19 — High Court odkazuje zejména na respektování lidské důstojnosti a osobní svobodu (preambule), osobní autonomii (čl. 40 odst. 3, body 1 a 2), nedotknutelnost obydlí (čl. 40 odst. 5) a ochranu rodinného života (článek 41).

39. High Court tudíž uvádí, že kdyby projednávaná věc měla být rozhodnuta výlučně na základě irského práva, vyvstal by závažný problém v souvislosti s otázkou, zda Spojené státy „zajišťují odpovídající úroveň ochrany soukromí a základních práv a svobod“ ve smyslu čl. 11 odst. 1 zákona o ochraně osobních údajů. Z toho vyplývá, že na základě irského práva, konkrétně požadavků plynoucích z jeho ústavy, nemohl Komisař zamítnout stížnost M. Schremse, ale měl tuto otázku posoudit.

40. High Court však konstatuje, že se věc, která mu byla předložena, týká uplatňování unijního práva ve smyslu čl. 51 odst. 1 Listiny, takže by legalita rozhodnutí Komisaře měla být posuzována z hlediska unijního práva.

41. Problém, s nímž se Komisař potýká, vysvětlil High Court následovně. Podle čl. 11 odst. 2 písm. a) zákona o ochraně osobních údajů musí Komisař rozhodnout o otázce odpovídající ochrany ve třetích zemích „v souladu“ se zjištěním Unie, které učiní Komise na základě čl. 25 odst. 6 směrnice 95/46. Z toho plyne, že se Komisař nemůže od tohoto zjištění odchýlit. Vzhledem k tomu, že Komise v rozhodnutí 2000/520 konstatovala, že Spojené státy zajišťují odpovídající úroveň ochrany v souvislosti se zpracováním osobních údajů společnostmi, které přijmou zásady „bezpečného přístavu“, Komisař musí nutně zamítnout stížnost, v níž se poukazuje na neodpovídající úroveň takovéto ochrany.

42. High Court konstatuje, že se Komisař úzkostlivě držel znění směrnice 95/46 a rozhodnutí 2000/520, avšak zároveň podotýká, že M. Schrems má ve skutečnosti výhrady spíše vůči podmínkám samotného režimu „bezpečného přístavu“ než vůči způsobu, jakým jej Komisař uplatnil, a zároveň zdůrazňuje, že M. Schrems přímo nezpochybnil platnost směrnice 95/46 ani platnost rozhodnutí 2000/520.

43. Podle High Court je tudíž zásadní otázka, zda je Komisař s ohledem na unijní právo a s přihlédnutím zejména k následnému nabytí účinnosti článků 7 a 8 Listiny absolutně vázán zjištěním Komise obsaženým v rozhodnutí 2000/520 ohledně odpovídajícího charakteru práva a praxe v oblasti ochrany osobních údajů ve Spojených státech.

44. High Court dále upřesňuje, že v žalobě, která mu byla předložena, nebyla uplatněna žádná výtka ohledně činností společností Facebook Ireland a Facebook USA jako takových. Článek 3 odst. 1 písm. b) rozhodnutí 2000/520, který příslušným vnitrostátním orgánům dovoluje, aby určité společnosti nařídily zastavit toky údajů do třetí země, se přitom podle tohoto soudu použije pouze v případě, kdy je stížnost namířena proti chování dotyčné společnosti, čemuž v projednávané věci není.

45. High Court tudíž zdůrazňuje, že skutečná námitka nesměřuje vůči chování společnosti Facebook USA jako takovému, ale spíše proti tomu, že Komise konstatovala, že právo a praxe v oblasti ochrany osobních údajů ve Spojených státech zajišťují odpovídající ochranu, přestože ze zjištění učiněných E. Snowdenem vychází jasně najevo, že americké orgány mohou mít rozsáhlý a nediferencovaný přístup k osobním údajům týkajícím se populace žijící na území Unie [20].

46. V této souvislosti je High Court názoru, že si lze jen stěží představit, jak by rozhodnutí 2000/520 mohlo v praxi splňovat požadavky stanovené články 7 a 8 Listiny tím spíše v případě, že se přihlédne k zásadám vytýčeným Soudním dvorem v rozsudku Digital Rights Ireland a další [21]. Konkrétně záruka zakotvená v článku 7 Listiny a základními hodnotami společnými tradicím členských států by byla popřena, kdyby byl orgánům veřejné moci umožněn nahodilý a globální přístup k elektronickým

20 — High Court v tomto ohledu uvádí, že hlavní žalobní důvod, který před ním uplatnil M. Schrems, spočívá v tvrzení, že vzhledem k nedávným zjištěním E. Snowdena a ke skutečnosti, že osobní údaje byly rozsáhle zpřístupněny zpravodajským službám Spojených států, nemohl Komisař důvodně dospět k závěru, že v této třetí zemi existuje odpovídající úroveň ochrany těchto údajů.

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

komunikacím bez jakéhokoli objektivního odůvodnění založeného na důvodech bezpečnosti státu nebo předcházení trestným činům, které se konkrétně vážou k dotyčným osobám, a bez jakýchkoli odpovídajících a ověřitelných záruk. Vzhledem k tomu, že žaloba M. Schremse naznačuje, že rozhodnutí 2000/520 by *in abstracto* mohlo být neslučitelné s články 7 a 8 Listiny, Soudní dvůr by mohl pokládat za možné vykládat směrnici 95/46, a konkrétně její čl. 25 odst. 6, jakož i rozhodnutí 2000/520 v tom smyslu, že by vnitrostátním orgánům umožňovaly provést vlastní šetření s cílem určit, zda předání osobních údajů do třetí země splňuje požadavky plynoucí z článků 7 a 8 Listiny.

47. Za těchto podmínek se High Court rozhodl přerušit řízení a položit Soudnímu dvoru následující předběžné otázky:

„Je s ohledem na články 7, 8 a 47 Listiny, aniž je dotčen čl. 25 odst. 6 směrnice 95/46, Komisař při posuzování stížnosti, která mu byla podána a podle které dochází k předávání osobních údajů do třetí země (v tomto případě do Spojených států), jejíž právní předpisy a praxe údajně nezajišťují odpovídající ochranu pro subjekty údajů, absolutně vázán opačným zjištěním Unie obsaženým v rozhodnutí 2000/520?

Nebo v opačném případě může či musí Komisař provést ve věci vlastní šetření s ohledem na vývoj faktické situace, ke kterému došlo od prvotního zveřejnění rozhodnutí 2000/520?“

## II – **Analýza**

48. Obě otázky položené High Court vyzývají Soudní dvůr k upřesnění pravomocí, jimiž jsou nadány vnitrostátní orgány dozoru v případě, že je k nim podána stížnost týkající se předávání osobních údajů společnosti usazené ve třetí zemi, na jejíž podporu je uplatňováno tvrzení, že tato třetí země nezajišťuje odpovídající úroveň ochrany předávaných údajů, ačkoli Komise přijala na základě čl. 25 odst. 6 směrnice 95/46 rozhodnutí, v němž uznala odpovídající úroveň ochrany zajišťovanou uvedenou třetí zemí.

49. Podotýkám, že stížnost podaná M. Schremsem ke Komisaři je dvojího rozměru. Zpochybňuje předávání osobních údajů společností Facebook Ireland společnosti Facebook USA. M. Schrems se domáhá toho, aby toto předávání bylo zastaveno, neboť je názoru, že Spojené státy nezajišťují odpovídající úroveň ochrany osobních údajů předávaných v rámci režimu „bezpečného přístavu“. Konkrétně této třetí zemi vytýká, že zavedla program PRISM, jenž NSA umožňuje volný přístup k hromadným údajům uloženým na serverech umístěných ve Spojených státech. Stížnost se tedy konkrétně týká předávání osobních údajů společností Facebook Ireland společnosti Facebook USA, a zároveň obecně zpochybňuje úroveň ochrany těchto údajů zajišťovanou v rámci režimu „bezpečného přístavu“.

50. Komisař měl za to, že samotná existence rozhodnutí Komise, jež uznává, že Spojené státy zajišťují v rámci režimu „bezpečného přístavu“ odpovídající úroveň ochrany, mu brání v prošetření dané stížnosti.

51. Je tedy třeba společně posoudit obě otázky, jejichž účelem je v zásadě zjistit, zda článek 28 směrnice 95/46, ve spojení s články 7 a 8 Listiny musí být vykládán v tom smyslu, že existence rozhodnutí přijatého Komisí na základě čl. 25 odst. 6 této směrnice brání vnitrostátnímu orgánu dozoru v prošetření stížnosti, v níž se tvrdí, že třetí země nezajišťuje odpovídající úroveň ochrany předávaných osobních údajů, a případně v zastavení předávání těchto údajů.

52. Článek 7 Listiny zaručuje právo na respektování soukromého života, zatímco článek 8 Listiny výslovně zakotvuje právo na ochranu osobních údajů. Odstavce 2 a 3 posledně zmíněného článku upřesňují, že tyto údaje musí být zpracovány korektně, k přesně stanoveným účelům a na základě souhlasu dotčené osoby nebo na základě jiného oprávněného důvodu stanoveného zákonem, že každý má právo na přístup k údajům, které o něm byly shromážděny, a má právo na jejich opravu, a že na dodržování těchto pravidel dohlíží nezávislý orgán.

A – *K pravomocím vnitrostátních orgánů dozoru v případě rozhodnutí Komise o odpovídající úrovni ochrany*

53. Jak uvedl M. Schrems ve svém vyjádření, pro účely stížnosti dotčené v původním řízení je klíčová otázka předávání osobních údajů společností Facebook Ireland společnosti Facebook USA s ohledem na globální přístup NSA a dalších amerických bezpečnostních agentur k údajům uloženým u společnosti Facebook USA na základě pravomocí, které jim svěřují americké právní předpisy.

54. Vnitrostátní orgán dozoru, k němuž byla podána stížnost směřující ke zpochybnění zjištění, že třetí země zajišťuje odpovídající úroveň ochrany předávaných údajů, má podle M. Schremse pravomoc, disponuje-li důkazy svědčícími o opodstatněnosti tvrzení obsažených v této stížnosti, nařídit zastavení předávání údajů ze strany společnosti označené v uvedené stížnosti.

55. S přihlédnutím k povinnostem Komisaře chránit základní práva M. Schremse tento tvrdí, že Komisař má nejen povinnost provést šetření, ale v případě, že stížnosti je vyhověno, i využít svých pravomocí k zastavení toků údajů mezi společnostmi Facebook Ireland a Facebook USA.

56. Komisař však stížnost zamítl na základě ustanovení zákona o ochraně osobních údajů, jež podávají výčet jeho pravomocí. Tento závěr byl založen na stanovisku Komisaře, který byl vázán rozhodnutím 2000/520.

57. Z toho vyplývá, že ústředním problémem v projednávané věci je otázka, zda posouzení Komise ohledně odpovídající úrovně ochrany obsažené v rozhodnutí 2000/520 absolutně zavazuje vnitrostátní orgán pro ochranu osobních údajů a brání mu v prošetření tvrzení zpochybňujících toto zjištění. Předběžné otázky se tedy týkají rozsahu vyšetřovacích pravomocí vnitrostátních orgánů pro ochranu osobních údajů v případě, že Komise přijala rozhodnutí konstatující odpovídající úroveň ochrany.

58. Podle Komise je třeba vzít v úvahu rozdělení pravomocí mezi Komisi a vnitrostátní orgány pro ochranu osobních údajů. Pravomoci posledně zmíněných orgánů jsou zaměřeny na uplatňování právních předpisů v této oblasti v individuálních případech, kdežto obecný přezkum uplatňování rozhodnutí 2000/520, včetně každého rozhodnutí zahrnujícího pozastavení jeho uplatňování nebo jeho zrušení, spadá do pravomoci Komise.

59. Komise tvrdí, že M. Schrems neuplatnil konkrétní argumenty, jež by nasvědčovaly tomu, že mu hrozí bezprostřední riziko vzniku vážné škody z důvodu předání údajů společností Facebook Ireland společnosti Facebook USA. Naopak obavy vyjádřené M. Schremsem ohledně programů pro sledování vytvořených americkými bezpečnostními agenturami jsou z důvodu jejich abstraktnosti a obecnosti totožné s obavami, které vedly Komisi k zahájení přezkumu rozhodnutí 2000/520.

60. Komise je názoru, že kdyby vnitrostátní orgány dozoru přijímaly opatření na základě stížností, v nichž jsou vyjádřeny pouze strukturální a abstraktní obavy, zasahovaly by tím do pravomocí Komise k novému vyjednání podmínek tohoto rozhodnutí se Spojenými státy, nebo případně k pozastavení uplatňování tohoto rozhodnutí.

61. Osobně nesdílím názor Komise. Existence rozhodnutí přijatého Komisí na základě čl. 25 odst. 6 směrnice 95/46 nemůže podle mého názoru popřít ani omezit pravomoci, jimiž jsou nadány vnitrostátní orgány dozoru podle článku 28 této směrnice. Na rozdíl od toho, co tvrdí Komise, jsou-li k vnitrostátním orgánům dozoru podány individuální stížnosti, nebrání jim to podle mého názoru v tom, aby si na základě svých vyšetřovacích pravomocí a nezávislosti učinily vlastní úsudek o obecné úrovni ochrany zajišťované třetí zemí a vyvodily z toho při rozhodování v individuálních případech patřičné důsledky.

62. Z ustálené judikatury Soudního dvora vyplývá, že je při výkladu ustanovení unijního práva třeba zohlednit nejen jejich znění, ale i kontext, ve kterém se nachází, a cíle sledované právní úpravou, jíž jsou součástí [22].

63. Z bodu 62 odůvodnění směrnice 95/46 vyplývá, že „zřízení orgánů dozoru v členských státech vykonávajících zcela nezávisle své úkoly je zásadním prvkem ochrany osob v souvislosti se zpracováním osobních údajů“.

64. Podle čl. 28 odst. 1 prvního pododstavce této směrnice „[k]aždý členský stát pověří jeden nebo několik orgánů veřejné moci na svém území dohledem nad dodržováním předpisů přijatých členskými státy na základě této směrnice“. Článek 28 odst. 1 druhý pododstavec uvedené směrnice stanoví, že „[t]yto orgány plní úkoly, kterými jsou pověřeny, zcela nezávisle“.

65. Článek 28 odst. 3 směrnice 95/46 podává výčet pravomocí orgánů dozoru, a sice pravomoci provádět šetření, pravomoci účinně zasáhnout, jež jim umožňují zejména dočasně nebo trvale zakázat zpracování údajů, jakož i pravomoc obrátit se na soud v případě porušení vnitrostátních předpisů přijatých k provedení této směrnice nebo pravomoc oznámit tato porušení soudním orgánům.

66. Dále podle čl. 28 odst. 4 prvního pododstavce směrnice 95/46 se „[n]a orgán dozoru […] může obrátit jakákoli osoba […] se žádostí týkající se ochrany svých práv a svobod v souvislosti se zpracováním osobních údajů“. Článek 28 odst. 4 druhý pododstavec této směrnice upřesňuje, že „[n]a orgán dozoru se může zejména obrátit kdokoli s žádostí o ověření přípustnosti zpracování, pokud se uplatní vnitrostátní předpisy přijaté na základě článku 13 [uvedené] směrnice.“ Je nutno dodat, že posledně zmíněné ustanovení umožňuje členským státům přijmout legislativní opatření s cílem omezit rozsah několika povinností a práv stanovených ve směrnici 95/46, pokud toto omezení představuje opatření nezbytné pro zajištění zejména bezpečnosti státu, obrany, veřejné bezpečnosti, předcházení trestným činům a jejich vyšetřování, odhalování a stíhání.

67. Jak již Soudní dvůr uvedl, požadavek dohledu ze strany nezávislého orgánu nad dodržováním unijních pravidel na ochranu fyzických osob v souvislosti se zpracováním osobních údajů vyplývá rovněž z unijního primárního práva a konkrétně z čl. 8 odst. 3 Listiny a čl. 16 odst. 2 SFEU [23]. Rovněž připomněl, že „[z]řízení nezávislých orgánů dozoru v členských státech tedy představuje zásadní prvek ochrany osob v souvislosti se zpracováním osobních údajů“ [24].

22 — Viz zejména rozsudek Koushkaki (C-84/12, EU:C:2013:862, bod 34 a citovaná judikatura).

23 — Viz rozsudky Komise v. Rakousko (C-614/10, EU:C:2012:631, bod 36) a Komise v. Maďarsko (C-288/12, EU:C:2014:237, bod 47).

24 — Viz zejména rozsudek Komise v. Maďarsko (C-288/12, EU:C:2014:237, bod 48 a citovaná judikatura). V tomto smyslu viz též rozsudek Digital Rights Ireland a další (C-293/12 a C-594/12, EU:C:2014:238, bod 68 a citovaná judikatura).

68. Soudní dvůr již také judikoval, že „čl. 28 odst. 1 druhý pododstavec směrnice 95/46 musí být vykládán v tom smyslu, že orgány dozoru příslušné dohlížet na zpracování osobních údajů musí požívat nezávislosti, která jim umožní plnit jejich úkoly bez vnějšího vlivu. Tato nezávislost vylučuje zejména jakékoliv příkazy a jakýkoliv jiný vnější vliv v jakékoliv podobě, ať již přímý či nepřímý, které by mohly usměrňovat jejich rozhodnutí, a ohrozit tak plnění úkolu, který spočívá v zajištění spravedlivé rovnováhy mezi ochranou práva na soukromí a volným pohybem osobních údajů, uvedenými orgány“ [25].

69. Soudní dvůr rovněž upřesnil, že „[z]áruka nezávislosti vnitrostátních orgánů dozoru má zajistit účinnost a spolehlivost dohledu nad dodržováním předpisů v oblasti ochrany fyzických osob v souvislosti se zpracováním osobních údajů“ [26]. Tato záruka byla stanovena „s cílem posílit ochranu osob a organizací, kterých se […] rozhodnutí [těchto vnitrostátních orgánů dozoru] týkají“ [27].

70. Jak vyplývá zejména z bodu 10 odůvodnění a z článku 1 směrnice 95/46, má tato směrnice za cíl zajištění „vysoké úrovně ochrany základních práv a svobod v souvislosti se zpracováním osobních údajů“ v Unii [28]. Podle Soudního dvora jsou „[o]rgány dozoru uvedené v článku 28 směrnice 95/46 […] tedy strážci uvedených základních práv a svobod“ [29].

71. Vzhledem k významu úlohy vnitrostátních orgánů dozoru v oblasti ochrany fyzických osob v souvislosti se zpracováním osobních údajů nemohou být jejich intervenční pravomoci omezeny, a to i když Komise přijala rozhodnutí na základě čl. 25 odst. 6 směrnice 95/46.

72. V této souvislosti je nutno poznamenat, že nic nenasvědčuje tomu, že by režimy předávání osobních údajů do třetích zemí byly vyňaty z věcné působnosti článku 8 odst. 3 Listiny, který zakotvuje na nejvyšší hierarchické úrovni unijních právních norem význam dohledu nezávislého orgánu nad dodržováním pravidel pro ochranu osobních údajů.

73. Kdyby vnitrostátní orgány dozoru byly absolutně vázány rozhodnutími Komise, omezovalo by to nevyhnutelně jejich naprostou nezávislost. V souladu s jejich úlohou strážce základních práv musí mít vnitrostátní orgány dozoru možnost prošetřit zcela nezávisle stížnosti, které jsou k nim podány, ve vyšším zájmu ochrany fyzických osob v souvislosti se zpracováním osobních údajů.

74. Jak na jednání správně uvedly belgická vláda a Evropský parlament, mezi kapitolou IV směrnice 95/46 týkající se předávání osobních údajů do třetích zemí a kapitolou VI této směrnice, která se věnuje zejména úloze vnitrostátních orgánů dozoru, neexistuje žádný hierarchický vztah. Nic v této kapitole VI nenaznačuje, že by ustanovení týkající se vnitrostátních orgánů dozoru byla jakkoli podřízena odlišným ustanovením o předávání údajů obsaženým v kapitole IV směrnice 95/46.

75. Z článku 25 odst. 1 této směrnice, obsaženého v její kapitole IV, naopak vyplývá, že povolení k předávání osobních údajů do třetí země zajišťující odpovídající úroveň ochrany platí pouze s výhradou dodržování vnitrostátních předpisů přijatých na základě ostatních ustanovení uvedené směrnice.

25 — Viz zejména rozsudek Komise v. Maďarsko (C-288/12, EU:C:2014:237, bod 51 a citovaná judikatura).

26 — Rozsudek Komise v. Německo (C-518/07, EU:C:2010:125, bod 25).

27 — Tamtéž.

28 — Tamtéž (bod 22 a citovaná judikatura).

29 — Tamtéž (bod 23). V tomto smyslu viz též rozsudky Komise v. Rakousko (C-614/10, EU:C:2012:631, bod 52) a Komise v. Maďarsko (C-288/12, EU:C:2014:237, bod 53).

76. V této souvislosti připomínám, že podle uvedeného ustanovení musí členské státy ve svých vnitrostátních předpisech stanovit, že k předávání osobních údajů, které jsou předmětem zpracování nebo které mají být předmětem zpracování po předání, do třetích zemí může dojít, aniž by tím bylo dotčeno dodržování vnitrostátních předpisů přijatých na základě ostatních ustanovení směrnice 95/46, pouze pokud dotyčná třetí země zajistí odpovídající úroveň ochrany.

77. Podle čl. 28 odst. 1 této směrnice jsou vnitrostátní orgány dozoru pověřeny dohledem nad dodržováním předpisů přijatých členskými státy na základě uvedené směrnice na jejich území.

78. Při porovnání těchto dvou ustanovení lze konstatovat, že pravidlo stanovené v čl. 25 odst. 1 směrnice 95/46, podle kterého může k předávání osobních údajů dojít pouze tehdy, pokud třetí země, do níž jsou údaje předávány, zajišťuje odpovídající úroveň ochrany těchto údajů, je součástí pravidel, jejichž dodržování podléhá dohledu ze strany vnitrostátních orgánů dozoru.

79. V souladu s čl. 8 odst. 3 Listiny je třeba pravomoci vnitrostátních orgánů dozoru ke zcela nezávislému prošetření stížností, které jsou k nim podány na základě článku 28 směrnice 95/46, vykládat široce. Tyto pravomoci tedy nemohou být omezeny pravomocemi, které unijní normotvůrce svěřil na základě čl. 25 odst. 6 uvedené směrnice Komisi, za účelem konstatování odpovídající úrovně ochrany poskytované třetí zemí.

80. Vzhledem k jejich zásadní úloze v oblasti ochrany osobních údajů musí mít vnitrostátní orgány dozoru možnost prošetřit k nim podanou stížnost, v níž jsou tvrzeny skutečnosti, jež by mohly zpochybnit úroveň ochrany zajišťované třetí zemí, a to včetně případu, kdy Komise v rozhodnutí přijatém na základě čl. 25 odst. 6 směrnice 95/46 konstatovala, že dotyčná třetí země zajišťuje odpovídající úroveň ochrany.

81. Pokud vnitrostátní orgán dozoru dospěje po provedení šetření k názoru, že sporné předání údajů narušuje ochranu, která náleží unijním občanům v souvislosti se zpracováním jejich údajů, má tento orgán pravomoc předmětné předávání údajů zastavit, a to bez ohledu na obecné posouzení učiněné Komisí v jejím rozhodnutí.

82. Podle čl. 25 odst. 2 směrnice 95/46 je totiž nesporné, že se odpovídající úroveň ochrany poskytovaná třetí zemí posoudí s ohledem na všechny skutkové a právní okolnosti. Pokud se některá z těchto okolností změní a jeví se, že by mohla zpochybnit odpovídající úroveň ochrany poskytované třetí zemí, musí mít vnitrostátní orgán dozoru, k němuž byla stížnost podána, možnost vyvodit z toho patřičné důsledky pro sporné předávání.

83. Jak uvedlo Irsko, Komisař je stejně jako jiné státní orgány vpravdě vázán rozhodnutím 2000/520. Z článku 288 čtvrtého pododstavce SFEU totiž vyplývá, že rozhodnutí přijatá unijními orgány jsou závazná v celém rozsahu. Rozhodnutí 2000/520 je tedy závazné pro členské státy, kterým je určeno.

84. V této souvislosti je nutno podotknout, že samo rozhodnutí 2000/520 v článku 5 stanoví, že „[č]lenské státy přijmou veškerá opatření nezbytná pro dosažení souladu s tímto rozhodnutím nejpozději do 90 dnů ode dne jeho oznámení členským státům“. Kromě toho článek 6 tohoto rozhodnutí potvrzuje, že „[t]oto rozhodnutí je určeno členským státům“.

85. Jsem však názoru, že s ohledem na výše uvedená ustanovení směrnice 95/46 a Listiny není závazný účinek rozhodnutí 2000/520 s to vyloučit jakékoli šetření ze strany Komisaře ohledně stížností, v nichž se tvrdí, že předávání osobních údajů do Spojených států v rámci tohoto rozhodnutí neposkytuje nutné záruky ochrany požadované unijním právem. Jinými slovy, takový závazný účinek není s to založit povinnost, aby každá stížnost tohoto druhu byla bez dalšího zamítnuta, to znamená neprodleně a bez jakéhokoli přezkumu její opodstatněnosti.

86. Dodávám, že ze struktury článku 25 směrnice 95/46 navíc vyplývá, že zjištění, podle něhož určitá třetí země zajišťuje, či nezajišťuje odpovídající úroveň ochrany, mohou učinit buď členské státy, nebo Komise. Jedná se tudíž o sdílenou pravomoc.

87. Z článku 25 odst. 6 této směrnice vyplývá, že jakmile Komise konstatuje, že třetí země zajišťuje odpovídající úroveň ochrany ve smyslu čl. 25 odst. 2 uvedené směrnice, členské státy musí přijmout opatření nezbytná pro dosažení souladu s rozhodnutím Komise.

88. Vzhledem k tomu, že účinkem tohoto rozhodnutí je umožnit předávání osobních údajů do třetí země, jejíž úroveň ochrany považuje Komise za odpovídající, členské státy tedy musí v zásadě umožnit tato předání ze strany společností usazených na jejich území.

89. Článek 25 směrnice 95/46 nepřiznává však Komisi výlučnou pravomoc ke zjištění odpovídající, či neodpovídající úrovně ochrany předávaných osobních údajů. Struktura tohoto článku svědčí o tom, že členské státy zaujímají v této oblasti též určitou roli. Rozhodnutí Komise má zajisté významnou úlohu při sjednocování podmínek pro předávání údajů platných v členských státech. Toto sjednocování však může přetrvávat pouze tak dlouho, dokud není toto zjištění zpochybněno.

90. Argument vycházející z nutnosti sjednocení podmínek pro předávání osobních údajů do třetí země ztrácí podle mého názoru své opodstatnění v takovém případě jako v původním řízení, kdy nejen že Komisi je známo, že proti jejímu zjištění existují výhrady, ale kdy tyto výhrady uplatnila sama Komise a vede jednání za účelem jejich napravení.

91. Posouzení odpovídající či neodpovídající úrovně ochrany poskytované třetí zemí může vést též ke spolupráci členských států s Komisí. Článek 25 odst. 3 směrnice 95/46 v tomto ohledu stanoví, že „[č]lenské státy a Komise se vzájemně informují o případech, kdy se domnívají, že některá třetí země nezajišťuje odpovídající úroveň ochrany ve smyslu odstavce 2“. Jak uvedl Parlament, tato skutečnost jasně svědčí o tom, že členské státy a Komise mají při odhalování případů, kdy některá třetí země nezajišťuje odpovídající úroveň ochrany, rovnocennou úlohu.

92. Účelem rozhodnutí o odpovídající úrovni ochrany je dovolit předávání osobních údajů do dotyčné třetí země. To neznamená, že se unijní občané již nemohou obrátit na orgány dozoru se žádostí o ochranu svých osobních údajů. V této souvislosti je nutno podotknout, že čl. 28 odst. 4 první pododstavec směrnice 95/46, podle kterého se „[n]a orgán dozoru […] může obrátit jakákoli osoba […] se žádostí týkající se ochrany svých práv a svobod v souvislosti se zpracováním osobních údajů“, nepřipouští z této zásady žádnou výjimku pro případ, že by Komise přijala rozhodnutí na základě čl. 25 odst. 6 této směrnice.

93. Ačkoli má rozhodnutí přijaté Komisí na základě prováděcích pravomocí, které jí přiznává posledně zmíněné ustanovení, za účinek umožnit předávání osobních údajů do třetí země, toto rozhodnutí nemůže naopak vést k tomu, že členské státy, a konkrétně jejich vnitrostátní orgány dozoru, budou v případě, že čelí tvrzením poukazujícím na porušení základních práv, zbaveny veškerých pravomocí, ba ani k tomu, že budou jim svěřené pravomoci omezeny.

94. Vnitrostátní orgán dozoru musí mít možnost vykonávat pravomoci stanovené v čl. 28 odst. 3 směrnice 95/46, včetně pravomoci dočasně nebo trvale zakázat zpracování osobních údajů. Ačkoli výčet pravomocí obsažený v tomto ustanovení výslovně neuvádí pravomoci související s předáváním osobních údajů z členského státu do třetí země, takové předávání musí být podle mého názoru

považováno za zpracování osobních údajů [30]. Jak vyplývá ze znění uvedeného ustanovení, tento výčet není navíc taxativní. S ohledem na zásadní úlohu vnitrostátních orgánů dozoru v systému zavedeném směrnicí 95/46 musí být tyto orgány každopádně nadány pravomocí k zastavení předávání údajů v případě prokázaného nebo potenciálního zásahu do základních práv.

95. Je nutno dodat, že by odepření pravomocí vnitrostátního orgánu dozoru provést šetření za takových okolností jako v projednávané věci bylo v rozporu nejen se zásadou nezávislosti, ale i s cílem směrnice 95/46, který vyplývá z jejího čl. 1 odst. 1.

96. Soudní dvůr poukázal na to, že „[z] bodů 3, 8 a 10 odůvodnění směrnice 95/46 vyplývá, že unijní normotvůrce měl v úmyslu sblížením právních předpisů členských států usnadnit volný pohyb osobních údajů a zároveň chránit základní práva jednotlivců, zejména právo na ochranu soukromí, a zajistit vysokou úroveň ochrany v Unii. Článek 1 této směrnice v tomto ohledu stanoví, že členské státy musí zajistit ochranu základních práv a svobod fyzických osob, zejména jejich soukromí, v souvislosti se zpracováním osobních údajů“ [31].

97. Ustanovení směrnice 95/46 musí být tedy vykládána v souladu s cílem této směrnice, jímž je zaručit vysokou úroveň ochrany základních práv a svobod fyzických osob, zejména jejich soukromí, v souvislosti se zpracováním osobních údajů v rámci Unie.

98. Význam tohoto cíle a úloha členských států při jeho naplňování znamenají, že vyvstanou-li zvláštní okolnosti zakládající vážnou pochybnost o respektování základních práv zaručených Listinou v případě předávání osobních údajů do třetí země, nemohou být členské státy, a tudíž v rámci nich vnitrostátní orgány dozoru absolutně vázány rozhodnutím Komise o odpovídající úrovni ochrany.

99. Soudní dvůr již judikoval, že „ustanovení směrnice 95/46 musí být v rozsahu, v němž upravují zpracování osobních údajů, které může představovat zásah do základních svobod, a zejména práva na soukromí, nutně vykládána ve světle základních práv, která podle ustálené judikatury tvoří nedílnou součást obecných právních zásad, jejichž dodržování Soudní dvůr zajišťuje a která jsou nyní zakotvená v Listině [32].

100. Dále odkazuji na judikaturu, podle níž „musí členské státy nejen vykládat své vnitrostátní právo v souladu s unijním právem, ale rovněž dbát na to, aby se neopíraly o výklad znění předpisu sekundárního práva, který koliduje se základními právy chráněnými unijním právním řádem nebo s jinými obecnými zásadami unijního práva“ [33].

101. Soudní dvůr v tomto ohledu v rozsudku N. S. a další [34] rozhodl, že „použití nařízení [(ES)] č. 343/2003[ [35]] na základě nevyvratitelné domněnky, že základní práva žadatele o azyl budou v členském státě primárně příslušném k posouzení jeho žádosti o azyl dodržována, je neslučitelné s povinností členských států vykládat a uplatňovat nařízení č. 343/2003 v souladu se základními právy“ [36].

30 — Viz stanovisko generálního advokáta P. Légera ve věci Parlament v. Rada a Komise (C-317/04, EU:C:2005:710, body 92 až 95). Viz též rozsudek Parlament v. Rada a Komise (C-317/04 a C-318/04, EU:C:2006:346, bod 56).

31 — Viz zejména rozsudek IPI (C-473/12, EU:C:2013:715, bod 28 a citovaná judikatura).

32 — Viz zejména rozsudek Google Spain a Google (C-131/12, EU:C:2014:317, bod 68 a citovaná judikatura).

33 — Viz zejména rozsudek N. S. a další (C-411/10 a C-493/10, EU:C:2011:865, bod 77 a citovaná judikatura).

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

35 — Nařízení Rady ze dne 18. února 2003, kterým se stanoví kritéria a postupy pro určení členského státu příslušného k posuzování žádosti o azyl podané státním příslušníkem třetí země v některém z členských států (Úř. věst. L 50, s. 1; Zvl. vyd. 19/06, s. 109).

36 — Bod 99 tohoto rozsudku.

102. V tomto ohledu Soudní dvůr v kontextu statusu členských států jako navzájem se považujících pro veškeré právní a praktické účely spojené se záležitostmi azylu za bezpečné země, uznal, že je třeba předpokládat, že zacházení s žadateli o azyl v každém členském státě splňuje požadavky Listiny, Úmluvy o právním postavení uprchlíků, podepsané v Ženevě dne 28. července 1951[37], a Evropské úmluvy o ochraně lidských práv a základních svobod, podepsané v Římě dne 4. listopadu 1950[38]. Soudní dvůr však rozhodl, že „[n]elze […] vyloučit, že tento systém v praxi naráží v určitém členském státě na závažné funkční problémy, takže existuje vážné riziko, že žadatelé o azyl budou v případě přemístění do tohoto členského státu vystaveni zacházení, které je neslučitelné s jejich základními právy“[39].

103. Soudní dvůr proto rozhodl, že „členské státy, včetně vnitrostátních soudů, nemohou přemístit žadatele o azyl do ‚příslušného členského státu' ve smyslu nařízení č. 343/2003, nemohou-li ponechat bez povšimnutí skutečnost, že systémové nedostatky azylového řízení a podmínek přijímání žadatelů o azyl v tomto členském státě představují závažné a prokazatelné důvody pro domněnku, že žadatel bude vystaven skutečnému riziku nelidského nebo ponižujícího zacházení ve smyslu článku 4 Listiny“[40].

104. Poznatky plynoucí z rozsudku N. S. a další[41] lze podle mého názoru vztáhnout i na takový případ, o jaký jde v původním řízení. Takový výklad unijního sekundárního práva, který by spočíval na nevyvratitelné domněnce, že základní práva budou respektována – ať již členským státem, Komisí nebo třetí zemí – musí být tedy považován za neslučitelný s povinností členských států vykládat a uplatňovat unijní sekundární právo v souladu se základními právy. Článek 25 odst. 6 směrnice 95/46 tudíž nestanoví takovouto nevyvratitelnou domněnku respektování základních práv v souvislosti s posouzením odpovídající úrovně ochrany poskytované třetí zemí ze strany Komise. Naopak domněnka, na které toto ustanovení spočívá, že při předávání údajů do určité třetí země jsou respektována základní práva, musí být považována za vyvratitelnou[42]. Uvedené ustanovení by tudíž nemělo být vykládáno v tom smyslu, že zpochybňuje záruky obsažené zejména v čl. 28 odst. 3 směrnice 95/46 a v čl. 8 odst. 3 Listiny, jež mají zajistit ochranu a dodržování práva na ochranu osobních údajů.

105. Z výše uvedeného rozsudku tedy lze dovodit, že v případě systémových nedostatků zjištěných ve třetí zemi, do které jsou osobní údaje předávány, musí mít členské státy možnost přijmout opatření nezbytná k ochraně základních práv chráněných články 7 a 8 Listiny.

106. Jak navíc uvedla ve svém vyjádření italská vláda, přijetí rozhodnutí o odpovídající úrovni ochrany Komisí nemůže mít za účinek snížení ochrany unijních občanů v souvislosti se zpracováním jejich osobních údajů v případě, že tyto údaje jsou předávány do třetí země, oproti úrovni ochrany, které by tyto osoby požívaly, kdyby jejich osobní údaje byly zpracovány v rámci Unie. Vnitrostátní orgány dozoru tudíž musí být s to zasáhnout a využít svých pravomocí v souvislosti s předáváním osobních údajů do třetích zemí, na které se vztahuje rozhodnutí o odpovídající úrovni ochrany. V opačném případě by unijní občané byli chráněni méně než v případě zpracování jejich osobních údajů v rámci Unie.

107. Jediným účinkem přijetí rozhodnutí Komisí na základě čl. 25 odst. 6 směrnice 95/46 je zrušení obecného zákazu vývozu osobních údajů do třetích zemí, které zajišťují srovnatelnou úroveň ochrany s úrovní poskytovanou touto směrnicí. Jinými slovy, nejedná se o vytvoření zvláštního režimu výjimek, který by unijním občanům poskytoval nižší ochranu oproti obecnému režimu stanovenému uvedenou směrnicí pro zpracování osobních údajů v rámci Unie.

37 — *Sbírka úmluv Organizace spojených národů*, sv. 189, s. 150, č. 2545 (1954).

38 — Viz rozsudek N. S. a další (C-411/10 a C-493/10, EU:C:2011:865, bod 80).

39 — Tamtéž (bod 81).

40 — Tamtéž (bod 94).

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

42 — Bod 104 tohoto rozsudku.

108. Soudní dvůr sice v bodě 63 rozsudku Lindqvist [43] uvedl, že „[k]apitola IV směrnice 95/46, v níž je obsažen článek 25, zavádí zvláštní režim“. To však podle mého názoru neznamená, že tento režim musí poskytovat nižší ochranu. Naopak článek 25 směrnice 95/46 ukládá za účelem dosažení cíle ochrany osobních údajů, stanoveného v čl. 1 odst. 1 této směrnice, členským státům a Komisi řadu povinností [44] a tentýž článek zakotvuje zásadu, podle které v případě, kdy třetí země neposkytuje odpovídající úroveň ochrany, musí být předávání osobních údajů do této země zakázáno [45].

109. Pokud jde konkrétně o režim „bezpečného přístavu“, Komise předpokládá zásah vnitrostátních orgánů dozoru a zastavení toků osobních údajů těmito orgány pouze v rámci vymezeném v čl. 3 odst. 1 písm. b) rozhodnutí 2000/520.

110. Podle bodu 8 odůvodnění tohoto rozhodnutí „[v] zájmu průhlednosti a proto, aby příslušné orgány v členských státech zajistily ochranu fyzických osob v souvislosti se zpracováním jejich osobních údajů, je nezbytné uvést v tomto rozhodnutí výjimečné okolnosti, za nichž může být odůvodněno pozastavení určitých toků údajů bez ohledu na zjištění odpovídající úrovně ochrany“.

111. V rámci projednávané věci bylo předmětem diskuze konkrétně použití čl. 3 odst. 1 písm. b) uvedeného rozhodnutí. Podle tohoto ustanovení mohou vnitrostátní orgány dozoru zastavit toky údajů, „pokud je velmi pravděpodobné, že zásady jsou porušovány; pokud se lze důvodně domnívat, že příslušný výkonný orgán včas nepřijal nebo nepřijme přiměřená opatření nezbytná pro vyřešení sporné věci; pokud by pokračování v předávání údajů vyvolalo bezprostřední riziko vzniku vážné újmy subjektům údajů a pokud příslušné orgány členského státu za daných okolností přiměřeně usilují o informování organizace a poskytly jí možnost zaujmout stanovisko“.

112. Uvedené ustanovení zakotvuje několik podmínek, jež byly předmětem různého výkladu ze strany účastníků řízení během probíhajícího řízení [46]. Aniž je třeba tyto výklady podrobně zkoumat, vyplývá z nich, že tyto podmínky striktně ohraničují pravomoc vnitrostátních orgánů dozoru k zastavení toků údajů.

113. Ačkoli Komise tvrdí opak, musí být čl. 3 odst. 1 písm. b) rozhodnutí 2000/520 vykládán v souladu s cílem ochrany osobních údajů, který sleduje směrnice 95/46, jakož i ve světle článku 8 Listiny. Požadavek výkladu v souladu se základními právy svědčí ve prospěch širokého výkladu tohoto ustanovení.

114. Z toho vyplývá, že podmínky stanovené v čl. 3 odst. 1 písm. b) rozhodnutí 2000/520 nemohou podle mého názoru bránit vnitrostátnímu orgánu dozoru ve zcela nezávislém výkonu pravomocí, které mu byly svěřeny na základě čl. 28 odst. 3 směrnice 95/46.

115. Jak na jednání v podstatě uvedly belgická a rakouská vláda, únikové východisko, které představuje čl. 3 odst. 1 písm. b) rozhodnutí 2000/520, je natolik úzké, že je v praxi realizovatelné jen stěží. Vyžaduje splnění kumulativních kritérií a staví laťku příliš vysoko. S ohledem na čl. 8 odst. 3 Listiny je přitom nemožné, aby rozhodovací prostor vnitrostátních orgánů dozoru ohledně výsad plynoucích z čl. 28 odst. 3 směrnice 95/46 byl omezen takovým způsobem, že těchto výsad již nebude možno využít.

43 — C-101/01, EU:C:2003:596.

44 — Bod 65.

45 — Bod 64.

46 — První podmínka, podle které „je velmi pravděpodobné, že zásady jsou porušovány“, není podle M. Schremse splněna. Není však tvrzeno, že společnost Facebook USA jakožto organizace s vlastním osvědčením, které jsou údaje předávány, sama porušila zásady bezpečného přístavu z důvodu rozsáhlého a nediferencovaného přístupu amerických orgánů k údajům, které má k dispozici. Zásady „bezpečného přístavu“ jsou totiž výslovně omezeny americkými právními předpisy, které příloha I čtvrtý pododstavec rozhodnutí 2000/520 definuje odkazem na zákon, správní nařízení nebo judikaturu.

116. Parlament v této souvislosti správně poznamenal, že o tom, jaké pravomoci mají být svěřeny vnitrostátním orgánům dozoru, rozhodl unijní normotvůrce. Prováděcí pravomoc přiznaná unijním normotvůrcem Komisi v čl. 25 odst. 6 směrnice 95/46 nezasahuje do pravomocí, které tentýž normotvůrce svěřil vnitrostátním orgánům dozoru v čl. 28 odst. 3 této směrnice. Jinými slovy, Komise není nadána pravomocí omezit pravomoci vnitrostátních orgánů dozoru.

117. V důsledku toho musí být vnitrostátní orgány dozoru k zajištění odpovídající ochrany základních práv fyzických osob v souvislosti se zpracováním osobních údajů oprávněny provést šetření v případě tvrzení poukazujících na porušení těchto práv. Dospějí-li uvedené orgány po provedení tohoto šetření k názoru, že v třetí zemi, na kterou se vztahuje rozhodnutí o odpovídající úrovni ochrany, existují závažné indicie, že jsou porušována práva unijních občanů na ochranu jejich osobních údajů, musí mít možnost zastavit předávání údajů subjektu usazenému v této třetí zemi.

118. Jinými slovy, vnitrostátní orgány dozoru musí mít možnost provést šetření, a případně zastavit předávání údajů, a to bez ohledu na restriktivní podmínky stanovené v čl. 3 odst. 1 písm. b) rozhodnutí 2000/520.

119. Kromě toho by vnitrostátní orgány dozoru na základě své pravomoci obrátit se na soud v případě porušení vnitrostátních předpisů přijatých k provedení směrnice 95/46 nebo pravomoci oznámit tato porušení soudním orgánům, stanovených v čl. 28 odst. 3 této směrnice, měly mít v případě, že jim jsou známy skutečnosti, které prokazují, že třetí země nezajišťuje odpovídající úroveň ochrany, možnost obrátit se na vnitrostátní soud, který sám bude moci případně rozhodnout o předložení žádosti o rozhodnutí o předběžné otázce Soudnímu dvoru za účelem posouzení platnosti rozhodnutí Komise o odpovídající úrovni ochrany.

120. Ze všech těchto poznatků vyplývá, že článek 28 směrnice 95/46, ve spojení s články 7 a 8 Listiny, musí být vykládán v tom smyslu, že existence rozhodnutí přijatého Komisí na základě čl. 25 odst. 6 této směrnice nebrání vnitrostátnímu orgánu dozoru v prošetření stížnosti, v níž se tvrdí, že třetí země nezajišťuje odpovídající úroveň ochrany předávaných osobních údajů, a případně v zastavení předávání těchto údajů.

121. Ačkoli High Court v předkládacím rozhodnutí zdůrazňuje, že M. Schrems v žalobě v původním řízení formálně nezpochybnil platnost směrnice 95/46 ani platnost rozhodnutí 2000/520, z tohoto předkládacího rozhodnutí vyplývá, že hlavní výhrada uplatněná M. Schremsem směřuje ke zpochybnění zjištění, že Spojené státy zajišťují v rámci režimu „bezpečného přístavu“ odpovídající úroveň ochrany předávaných osobních údajů.

122. Rovněž z vyjádření Komisaře vyplývá, že účelem stížnosti M. Schremse je přímo zpochybnit rozhodnutí 2000/520. Podáním této stížnosti měl M. Schrems v úmyslu napadnout podmínky a fungování režimu „bezpečného přístavu“ jako takového, a to protože rozsáhlé sledování osobních údajů předávaných do Spojených států svědčí o tom, že v právních předpisech a praxi platných v této třetí zemi neexistuje skutečná ochrana těchto údajů.

123. Předkládající soud navíc sám podotýká, že by záruka poskytovaná článkem 7 Listiny a základními hodnotami společnými ústavním tradicím členských států byla popřena, kdyby se orgánům veřejné moci umožnil nahodilý a globální přístup k elektronickým komunikacím bez poskytnutí jakéhokoli objektivního odůvodnění založeného na důvodech bezpečnosti státu nebo předcházení trestným činům, které se konkrétně vážou k dotyčným osobám, a bez jakýchkoli odpovídajících a ověřitelných záruk [47]. Předkládající soud tak nepřímo vyjadřuje pochybnosti o platnosti rozhodnutí 2000/520.

47 — Bod 24 předkládacího rozhodnutí.

124. Posouzení otázky, zda Spojené státy zajišťují v rámci režimu „bezpečného přístavu“ odpovídající úroveň ochrany předávaných údajů, tedy nutně vede k zamyšlení nad otázkou platnosti tohoto rozhodnutí.

125. V této souvislosti je třeba podotknout, že v rámci nástroje spolupráce mezi Soudním dvorem a vnitrostátními soudy, jenž byl zaveden článkem 267 SFEU, může Soudní dvůr, přestože mu byla předložena žádost o rozhodnutí o předběžné otázce týkající se výlučně výkladu unijního práva, považovat za určitých zvláštních okolností za nezbytné posoudit platnost ustanovení sekundárního práva.

126. Soudní dvůr tedy již několikrát prohlásil z úřední povinnosti akt, v jehož případě bylo žádáno pouze o jeho výklad, za neplatný [48]. Rovněž judikoval, že „pokud se jeví, že předmětem otázek položených vnitrostátním soudem je ve skutečnosti spíše přezkum platnosti než výklad aktů [Unie], Soudní dvůr podá uvedenému soudu neprodleně vysvětlení a nebude jej nutit ke splnění formálních požadavků, což by vedlo k průtahům v řízení neslučitelným se samotnou povahou mechanismů zakotvených článkem [267 SFEU]“ [49]. Soudní dvůr mimoto již shledal, že pochybnosti vyjádřené předkládajícím soudem ohledně slučitelnosti aktu sekundárního práva s pravidly pro ochranu základních práv musí být chápány jako zpochybňující platnost tohoto aktu z hlediska unijního práva [50].

127. Rovněž připomínám, že z judikatury Soudního dvora vyplývá, že se u aktů unijních orgánů, institucí a útvarů vychází z presumpce jejich platnosti, což znamená, že tyto akty vyvolávají právní účinky tak dlouho, dokud nejsou vzaty zpět, zrušeny v rámci žaloby na neplatnost nebo prohlášeny za neplatné v návaznosti na žádost o rozhodnutí o předběžné otázce nebo na námitku protiprávnosti. Rozhodnout o neplatnosti unijního aktu může pouze Soudní dvůr, přičemž cílem této pravomoci je zaručit právní jistotu prostřednictvím zajištění jednotného uplatňování unijního práva. Není-li rozhodnutí prohlášeno neplatným, změněno nebo zrušeno ze strany Komise, je nadále závazné v celém rozsahu a přímo použitelné ve všech členských státech [51].

128. Za účelem podání vyčerpávající odpovědi předkládajícímu soudu a rozptýlení pochybností vyjádřených během tohoto řízení ohledně platnosti rozhodnutí 2000/520 jsem názoru, že Soudní dvůr by tudíž měl posoudit platnost tohoto rozhodnutí.

129. Je však rovněž třeba upřesnit, že se posouzení otázky, zda rozhodnutí 2000/520 je, či není platné, musí omezit na výtky, jež byly předmětem diskuze v rámci tohoto řízení. V tomto rámci totiž nebyly projednány všechny aspekty týkající se fungování režimu „bezpečného přístavu“, a proto považuji za nemožné provést zde vyčerpávající přezkum nedostatků tohoto režimu.

130. Naproti tomu otázka, zda by globálním a necíleným přístupem amerických zpravodajských služeb k předávaným údajům mohla být dotčena legalita rozhodnutí 2000/520, byla projednána před Soudním dvorem v rámci tohoto řízení. Platnost tohoto rozhodnutí lze tedy posoudit z tohoto pohledu.

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

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

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

51 — Viz zejména rozsudek CIVAD (C-533/10, EU:C:2012:347, body 39 až 41 a citovaná judikatura).

B – *K platnosti rozhodnutí 2000/520*

1. Ke skutečnostem, které je třeba vzít v úvahu při posuzování platnosti rozhodnutí 2000/520

131. Je třeba připomenout judikaturu, podle které „musí být v rámci žaloby na neplatnost legalita aktu posuzována s ohledem na skutkové a právní okolnosti existující v okamžiku přijetí tohoto aktu, přičemž úsudek Komise lze kritizovat pouze tehdy, jeví-li se jako zjevně nesprávný z hlediska poznatků, jimiž disponovala v okamžiku přijetí dotčeného aktu“ [52].

132. Soudní dvůr v rozsudku Gaz de France – Berliner Investissement [53] připomněl zásadu, podle které „posouzení platnosti aktu, které Soudní dvůr provádí v rámci řízení o předběžné otázce, má být zpravidla založeno na situaci, která existuje v době přijetí aktu“ [54]. Soudní dvůr však patrně připustil, že „platnost aktu by mohla být v určitých případech posouzena s ohledem na nové skutečnosti, které nastaly až po jeho přijetí“ [55].

133. Tento otevřenější přístup takto nastíněný Soudním dvorem se mi zdá být v projednávané věci obzvláště relevantní.

134. Rozhodnutí přijatá Komisí na základě čl. 25 odst. 6 směrnice 95/46 totiž vykazují zvláštní znaky. Jsou určena k posouzení, zda úroveň ochrany osobních údajů poskytovaná určitou třetí zemí je odpovídající, či nikoliv. Toto posouzení se nutně mění v závislosti na skutkovém a právním kontextu v dotyčné třetí zemi.

135. Vzhledem k tomu, že rozhodnutí o odpovídající úrovni ochrany je zvláštním druhem rozhodnutí, je třeba pravidlo, podle kterého musí být posouzení platnosti tohoto rozhodnutí prováděno pouze s ohledem na okolnosti existující v době jeho přijetí, v projednávané věci relativizovat. Takovéto pravidlo by jinak vedlo k tomu, že by několik let po přijetí rozhodnutí o odpovídající úrovni ochrany nemohly být při posuzování platnosti, které musí provést Soudní dvůr, zohledněny události, které nastaly později, přestože pro podání žádosti o rozhodnutí o předběžné otázce týkající se platnosti neexistuje žádné časové omezení a její podání může být právě důsledkem pozdějších okolností, které svědčí o nedostatcích dotčeného aktu.

136. V projednávané věci svědčí zachování platnosti rozhodnutí 2000/520 po dobu přibližně patnácti let o tom, že Komise implicitně potvrdila své posouzení učiněné v roce 2000. Má-li Soudní dvůr v rámci řízení o předběžné otázce zkoumat platnost tohoto posouzení, na němž Komise stále trvá, je tedy nejen možné, ale i vhodné, aby toto posouzení zkoumal z hlediska nových okolností, které nastaly po přijetí rozhodnutí o odpovídající úrovni ochrany.

137. Rozhodnutí o odpovídající úrovni ochrany musí být vzhledem k jeho zvláštní povaze pravidelně přezkoumáváno ze strany Komise. Pokud v důsledku nových událostí, k nimž došlo v mezidobí, Komise své rozhodnutí nezmění, znamená to, že implicitně, ale nutně potvrzuje prvotní posouzení. Znovu tedy opakuje své zjištění, že dotyčná třetí země zajišťuje odpovídající úroveň ochrany předávaných osobních údajů. Je na Soudním dvoru, aby posoudil, zda navzdory pozdějším okolnostem je toto zjištění platné i nadále.

52 — Viz zejména rozsudek BVGD v. Komise (T-104/07 a T-339/08, EU:T:2013:366, bod 291), jenž odkazuje na rozsudek IECC v. Komise (C-449/98 P, EU:C:2001:275, bod 87).

53 — C-247/08, EU:C:2009:600.

54 — Bod 49 a citovaná judikatura.

55 — Bod 50 a citovaná judikatura. V tomto smyslu viz Lenaerts, K., Maselis, I., a Gutman, K., EU *Procedural Law*, Oxford University Press, 2014, kteří uvádí, 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).

138. Za účelem zajištění účinného soudního přezkumu tohoto druhu rozhodnutí musí být tedy při posuzování platnosti tohoto rozhodnutí podle mého názoru přihlédnuto k současnému skutkovému a právnímu kontextu.

2. K pojmu „odpovídající úroveň ochrany“

139. Článek 25 směrnice 95/46 plně spočívá na zásadě, podle které k předání osobních údajů do třetí země nemůže dojít, pokud tato třetí země nezajišťuje odpovídající úroveň ochrany těchto údajů. Cílem tohoto článku tedy je zajistit trvalou ochranu přiznanou touto směrnicí v případě předávání osobních údajů do určité třetí země. V tomto ohledu je třeba připomenout, že uvedená směrnice poskytuje vysokou úroveň ochrany unijních občanů v souvislosti se zpracováním jejich osobních údajů.

140. Vzhledem k důležité úloze ochrany osobních údajů z hlediska základního práva na respektování soukromí musí být tato vysoká úroveň ochrany tudíž zaručena i v případě předávání osobních údajů do třetí země.

141. Právě proto jsem názoru, že Komise může na základě čl. 25 odst. 6 směrnice 95/46 konstatovat, že třetí země zajišťuje odpovídající úroveň ochrany, pouze tehdy, když je po provedení celkového posouzení práva a praxe platných v dotyčné třetí zemi schopna určit, že tato třetí země poskytuje takovou úroveň ochrany, která je v zásadě rovnocenná úrovni poskytované touto směrnicí, přestože podmínky této ochrany se mohou lišit od těch, které běžně platí v rámci Unie.

142. Přestože anglický výraz „adequate“ může být z jazykového hlediska chápán jako označující úroveň ochrany, která je pouze uspokojivá či dostačující, a jeho sémantický obsah se tedy může lišit od francouzského výrazu „adéquat“, je třeba podotknout, že jediným kritériem, kterým je třeba se při výkladu tohoto pojmu řídit, je cíl spočívající v dosažení vysoké úrovně ochrany základních práv, který vyžaduje směrnice 95/46.

143. Přezkum úrovně ochrany poskytované třetí zemí se musí zaměřit na dva základní aspekty, a sice na obsah použitelných pravidel a prostředky k zajištění dodržování těchto pravidel [56].

144. K dosažení úrovně ochrany v zásadě rovnocenné úrovni poskytované v rámci Unie by režim „bezpečného přístavu“, který převážně spočívá na vlastním osvědčení a vlastním hodnocení společnostmi, jež se dobrovolně účastní tohoto režimu, měl být podle mého názoru doprovázen odpovídajícími zárukami a dostatečným kontrolním mechanismem. Na předávání osobních údajů do třetích zemí by se tak neměla vztahovat nižší ochrana než na zpracování prováděná v rámci Unie.

145. V této souvislosti je třeba předeslat, že v Unii převládá pojetí, podle něhož mechanismus vnější kontroly v podobě nezávislého orgánu představuje nezbytný prvek každého systému, jenž má zajišťovat dodržování pravidel pro ochranu osobních údajů.

146. Kromě toho je k zajištění užitečného účinku článku 25 odst. 1 až 3 směrnice 95/46 třeba přihlédnout k tomu, že odpovídající úroveň ochrany poskytované třetí zemí je vyvíjející se situací, která se může časem změnit v závislosti na řadě faktorů. Členské státy a Komise tedy musí soustavně věnovat pozornost jakékoli změně okolností, jež by si mohla vyžádat nové posouzení odpovídající úrovně ochrany poskytované třetí zemí. Posouzení odpovídající úrovně ochrany nemůže být v žádném případě zafixováno k pevně stanovenému okamžiku a následně být ponecháno v platnosti bez časového omezení nezávisle na jakékoli změně okolností svědčící o tom, že úroveň poskytované ochrany již ve skutečnosti není odpovídající.

56 — Viz s. 5 pracovního dokumentu Komise WP 12, nadepsaného „Předávání osobních údajů do třetích zemí: Uplatňování článků 25 a 26 směrnice o ochraně údajů“, přijatého pracovní skupinou pro ochranu fyzických osob v souvislosti se zpracováním osobních údajů dne 24. července 1998.

147. Závazek třetí země k zajištění odpovídající úrovně ochrany je tedy trvalým závazkem. Je-li provedeno posouzení k určitému okamžiku, zachování platnosti rozhodnutí o odpovídající úrovni ochrany předpokládá, že žádná okolnost, která od té doby nastane, nebude moci zpochybnit prvotní posouzení provedené Komisí.

148. Je totiž nutno mít stále na zřeteli, že cílem článku 25 směrnice 95/46 je zamezit tomu, aby osobní údaje byly předávány do třetí země, která nezajišťuje odpovídající úroveň ochrany, což je v rozporu se základním právem na ochranu osobních údajů zaručeným článkem 8 Listiny.

149. Je nutno zdůraznit, že pravomoc svěřená Komisi unijním normotvůrcem v čl. 25 odst. 6 směrnice 95/46 ke konstatování, že třetí země zajišťuje odpovídající úroveň ochrany, je výslovně podmíněna tím, že tato třetí země takovou úroveň ochrany ve smyslu odstavce 2 tohoto článku zajišťuje. Mohou-li nové okolnosti zpochybnit prvotní posouzení Komise, měla by Komise příslušným způsobem upravit své rozhodnutí.

3. Posouzení

150. Připomínám, že čl. 25 odst. 6 směrnice 95/46 uvádí, že „postupem podle čl. 31 odst. 2 Komise může konstatovat, že třetí země zajišťuje odpovídající úroveň ochrany ve smyslu odstavce 2 tohoto článku na základě svých vnitrostátních předpisů nebo mezinárodních závazků sjednaných zejména na závěr jednání uvedených v odstavci 5 s cílem zajistit ochranu soukromí a základních práv a svobod osob“. Článek 25 odst. 6 této směrnice vykládaný ve spojení s jejím čl. 25 odst. 2 znamená, že aby Komise mohla konstatovat, že třetí země zajišťuje odpovídající úroveň ochrany, musí provést celkové posouzení právních norem platných v této třetí zemi, jakož i jejich uplatňování.

151. Z výše uvedeného je patrné, že zachování platnosti rozhodnutí 2000/520 Komisí musí být navzdory výskytu nových skutkových a právních okolností chápáno jako vůle Komise potvrdit své prvotní posouzení.

152. Soudnímu dvoru nepřísluší, aby v rámci řízení o předběžné otázce posuzoval skutečnosti, z nichž vychází spor, jenž vedl vnitrostátní soud k podání žádosti o rozhodnutí o předběžné otázce [57].

153. Budu tedy vycházet ze skutečností, jež předkládající soud uvedl v žádosti o rozhodnutí o předběžné otázce, tedy skutečností, které navíc sama Komise uznala v široké míře za prokázané [58].

154. Skutečnosti, které byly uplatněny před Soudním dvorem ke zpochybnění posouzení Komise, podle něhož režim „bezpečného přístavu“ zajišťuje odpovídající úroveň ochrany osobních údajů předávaných z Unie do Spojených států, mohou být popsány následovně.

155. Předkládající soud vychází v žádosti o rozhodnutí o předběžné otázce z následujících dvou skutkových zjištění. Zaprvé osobní údaje předávané takovými společnostmi, jako je Facebook Ireland, jejich mateřské společnosti usazené ve Spojených státech mohou být následně konzultovány NSA a jinými americkými bezpečnostními agenturami v rámci rozsáhlých a necílených činností sledování a zachycování údajů. V návaznosti na zjištění E. Snowdena totiž nelze v současnosti dospět na základě dostupných důkazů k žádnému jinému přijatelnému závěru [59]. Zadruhé unijní občané nemají žádné účinné právo být vyslechnuti k otázce sledování a zachycování svých osobních údajů ze strany NSA a jiných amerických bezpečnostních agentur [60].

57 — Viz zejména rozsudek Fallimento Traghetti del Mediterraneo (C-140/09, EU:C:2010:335, bod 22 a citovaná judikatura).

58 — Viz sdělení Komise zmíněné v poznámce pod čarou 2 a sdělení Komise Evropskému parlamentu a Radě o fungování „bezpečného přístavu“ z pohledu občanů EU a společností usazených v EU [COM(2013) 847 final].

59 — Bod 7 písm. c) předkládacího rozhodnutí.

60 — Bod 7 písm. b) předkládacího rozhodnutí.

156. Tato skutková zjištění High Court jsou podložena zjištěními samotné Komise.

157. Ve výše zmíněném sdělení o fungování bezpečného přístavu z hlediska občanů EU a společností usazených v EU vycházela Komise ze zjištění, že v průběhu roku 2013 vyvolaly informace o množství a rozsahu amerických programů pro sledování údajů obavy o trvalou ochranu osobních údajů legálně předaných do Spojených států v rámci systému zásad „bezpečného přístavu“. Komise uvedla, že se zdá, že všechny společnosti zapojené do programu PRISM, které poskytují orgánům Spojených států přístup k údajům uchovávaným a zpracovávaným v USA, mají osvědčení o dodržování zásad „bezpečného přístavu“. To podle ní ze systému „bezpečného přístavu“ učinilo jednu z cest, jejichž prostřednictvím mají orgány zpravodajství Spojených států přístup k shromažďování osobních údajů původně zpracovávaných v Unii [61].

158. Z těchto poznatků vyplývá, že právo a praxe platné ve Spojených státech umožňují shromažďovat v rozsáhlé míře osobní údaje unijních občanů, které jsou předávány v rámci režimu „bezpečného přístavu“, aniž tito občané požívají účinné právní ochrany.

159. Tato skutková zjištění podle mého názoru dokládají, že rozhodnutí 2000/520 neobsahuje dostatečné záruky. Z důvodu chybějících záruk bylo toto rozhodnutí provedeno způsobem, který nesplňuje požadavky stanovené Listinou a směrnicí 95/46.

160. Účelem rozhodnutí přijatého Komisí na základě čl. 25 odst. 6 směrnice 95/46 je přitom konstatovat, že třetí země „zajišťuje“ odpovídající úroveň ochrany. Výraz „zajišťuje“ v přítomném čase znamená, že aby platnost tohoto rozhodnutí mohla být zachována, musí se týkat třetí země, která i po přijetí uvedeného rozhodnutí nadále zaručuje odpovídající úroveň ochrany.

161. Zjištění ohledně postupů NSA, která údajně využívá údaje předané v rámci režimu „bezpečného přístavu“, ve skutečnosti odkryla nedostatky právního základu, jejž představuje rozhodnutí 2000/520.

162. Nedostatky, na které bylo v průběhu tohoto řízení poukázáno, se konkrétně nacházejí v příloze I čtvrtém pododstavci tohoto rozhodnutí.

163. Připomínám, že podle uvedeného ustanovení „[d]održování […] zásad [bezpečného přístavu] může být omezeno: a) v rozsahu nezbytném pro splnění požadavků bezpečnosti státu, veřejného zájmu nebo prosazování zákonů Spojených států; b) zákonem, správním nařízením nebo judikaturou, které vytvářejí protichůdné závazky, nebo výslovným zmocněním za předpokladu, že při výkonu takového zmocnění může organizace prokázat, že nedodržení zásad je omezeno na rozsah nezbytný pro dodržení nadřazených oprávněných zájmů, jimž má takové zmocnění sloužit“.

164. Problém spočívá především v uplatňování výjimek stanovených v uvedeném ustanovení ze strany orgánů Spojených států. Z důvodu jejich příliš obecné formulace se uplatňování těchto výjimek uvedenými orgány neomezuje na nezbytně nutné.

165. K této příliš obecné formulaci přistupuje okolnost, že unijní občané nedisponují vhodnými procesními prostředky k obraně proti zpracování jejich osobních údajů za jinými účely, než jsou ty, pro které byly tyto údaje původně shromážděny a následně předány do Spojených států.

166. Výjimky stanovené v rozhodnutí 2000/520 z použití zásad „bezpečného přístavu“, zejména v rozsahu nezbytném pro splnění požadavků bezpečnosti státu, měly být doprovázeny zavedením nezávislého kontrolního mechanismu, jenž by zamezoval zjištěným zásahům do práva na soukromí.

61 — Strana 19 jejího sdělení.

167. Zjištění ohledně praktik amerických zpravodajských služeb v souvislosti s globálním sledováním údajů předávaných v rámci „bezpečného přístavu“ odkryla některé nedostatky specifické pro rozhodnutí 2000/520.

168. Z tvrzení uplatňovaných v projednávané věci neplyne, že by společnost Facebook porušila zásady „bezpečného přístavu“. Pokud taková společnost vlastnící osvědčení, jako je společnost Facebook USA, umožní americkým orgánům přístup k údajům, které jí byly předány z některého členského státu, lze konstatovat, že zmíněná společnost tak činí s cílem dosáhnout souladu s americkými právními předpisy. S ohledem na skutečnost, že rozhodnutí 2000/520 z důvodu široké formulace v něm obsažených výjimek takovýto případ výslovně připouští, otázkou, která v projednávané věci vyvstává, je ve skutečnosti otázka slučitelnosti těchto výjimek s unijním primárním právem.

169. V této souvislosti je třeba zdůraznit, že z ustálené judikatury Soudního dvora vyplývá, že respektování lidských práv je podmínkou legality unijních aktů a že v Unii nelze připustit opatření, která jsou neslučitelná s jejich dodržováním [62].

170. Z judikatury Soudního dvora dále vyplývá, že sdělení shromážděných osobních údajů třetím osobám, veřejným či soukromým, představuje zásah do práva na respektování soukromého života „nehledě na to, jak jsou později takto sdělené informace využity“ [63]. Kromě toho v rozsudku Digital Rights Ireland a další [64] Soudní dvůr potvrdil, že povolení přístupu k takovým údajům příslušným vnitrostátním orgánům je dalším zásahem do tohoto základního práva [65]. Navíc jakákoli podoba zpracování osobních údajů spadá pod článek 8 Listiny a představuje zásah do ochrany těchto údajů [66]. Přístup, který mají americké zpravodajské služby k předávaným údajům, tudíž rovněž představuje zásah do základního práva na ochranu osobních údajů zaručeného článkem 8 Listiny, neboť takovýto přístup představuje zpracování těchto údajů.

171. Obdobně tomu, co shledal Soudní dvůr v uvedeném rozsudku, takto zjištěný zásah je vzhledem k značnému množství dotčených uživatelů a kvantitě předávaných údajů velmi rozsáhlý, a musí být považován za zvlášť závažný. Tyto skutečnosti ve spojení s tajností přístupu amerických orgánů k osobním údajům předávaným společnostem usazeným ve Spojených státech činí zásah mimořádně závažným.

172. K tomu přistupuje okolnost, že unijní občané, kteří jsou uživateli Facebooku, nejsou informováni o tom, že jejich osobní údaje budou globálně přístupné americkým bezpečnostním agenturám.

173. Je rovněž třeba zdůraznit, že předkládající soud konstatoval, že unijní občané nemají ve Spojených státech žádné účinné právo být vyslechnuti k otázce sledování a zachycování svých údajů. FISC vykonává určitý dohled, avšak řízení před ním je tajné a nekontradiktorní [67]. Jsem názoru, že jde zde o zásah do práva unijních občanů na účinnou právní ochranu, chráněného článkem 47 Listiny.

174. Zásah, který umožňují výjimky ze zásad „bezpečného přístavu“ obsažené v příloze I čtvrtém pododstavci rozhodnutí 2000/520 do základních práv chráněných články 7, 8 a 47 Listiny, je tudíž prokázán.

175. Nyní je třeba ověřit, zda tento zásah je či není odůvodněný.

62 — Viz zejména rozsudek Kadi a Al Barakaat International Foundation v. Rada a Komise (C-402/05 P a C-415/05 P, EU:C:2008:461, bod 284 a citovaná judikatura).

63 — Rozsudek Österreichischer Rundfunk a další (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.

67 — Bod 7 písm. b) předkládacího rozhodnutí.

176. Podle čl. 52 odst. 1 Listiny musí být každé omezení výkonu práv a svobod zakotvených v Listině stanoveno zákonem a musí respektovat podstatu těchto práv a svobod. Při dodržení zásady proporcionality mohou být omezení těchto práv a svobod zavedena pouze tehdy, jsou-li nezbytná a odpovídají skutečně cílům obecného zájmu, které uznává Unie, nebo potřebě ochrany práv a svobod druhého.

177. S ohledem na takto stanovené podmínky k umožnění omezení výkonu práv a svobod chráněných Listinou mám silné pochybnosti o tom, že omezení, o která jde v projednávané věci, lze považovat za respektující podstatu článků 7 a 8 Listiny. Přístup amerických zpravodajských služeb k předaným údajům se totiž podle všeho vztahuje i na obsah elektronických komunikací, což zasahuje do podstaty základního práva na respektování soukromého života a dalších práv zakotvených v článku 7 Listiny. Navíc v rozsahu, v němž široká formulace omezení stanovených v příloze I čtvrtém pododstavci rozhodnutí 2000/520 potenciálně umožňuje vyloučit uplatnění všech zásad „bezpečného přístavu, lze mít za to, že tato omezení zasahují do podstaty základního práva na ochranu osobních údajů [68].

178. Pokud jde o otázku, zda zjištěný zásah odpovídá cíli obecného zájmu, předně připomínám, že podle přílohy I čtvrtého pododstavce písm. b) rozhodnutí 2000/520 může být dodržování zásad „bezpečného přístavu“ omezeno „zákonem, správním nařízením nebo judikaturou, které vytvářejí protichůdné závazky, nebo výslovným zmocněním za předpokladu, že při výkonu takového zmocnění může organizace prokázat, že nedodržení zásad je omezeno na rozsah nezbytný pro dodržení nadřazených oprávněných zájmů, jimž má takové zmocnění sloužit“.

179. Je nutno konstatovat, že „oprávněné zájmy“, na které toto ustanovení poukazuje, nejsou konkrétně upřesněny. Z toho vyplývá určitá nejistota ohledně potenciálně příliš široké působnosti této výjimky z použití zásad „bezpečného přístavu“ společnostmi, které tyto zásady přijaly.

180. Vysvětlení obsažená v části B přílohy IV rozhodnutí 2000/520, nadepsané „Výslovná právní zmocnění“, potvrzují tento dojem, konkrétně tvrzení, že „[j]e však jasné, že tam, kde právo Spojených států ukládá závazek odporující zásadám ‚bezpečného přístavu‘, je organizace ve Spojených státech povinna dodržovat toto právo bez ohledu na to, zda se účastní ‚bezpečného přístavu‘, nebo nikoli“. V souvislosti s výslovnými zmocněními se zde dále uvádí, že „zatímco zásady ‚bezpečného přístavu‘ mají za cíl překlenout rozdíly mezi úpravami ochrany soukromí v právním systému Spojených států a v evropském systému, musíme respektovat zákonodárné výhradní pravomoci našich zvolených zákonodárců“.

181. Z toho vyplývá, že tato výjimka je podle mého názoru v rozporu s články 7, 8 a čl. 52 odst. 1 Listiny, neboť nesleduje dostatečně konkrétně definovaný cíl obecného zájmu.

182. Snadnost a obecnost, s nimiž samo rozhodnutí 2000/520 v příloze I čtvrtém pododstavci písm. b) a v příloze IV části B stanoví, že se od zásad „bezpečného přístavu“ lze odchýlit na základě právních norem Spojených států, jsou každopádně neslučitelné s podmínkou, podle které se odchylky od pravidel v oblasti ochrany osobních údajů musí omezovat na nezbytně nutné. Podmínka nutnosti je vpravdě zmíněna, ale vedle toho, že prokázat splnění této podmínky musí dotyčná společnost, mi není jasné, jak by se tato společnost mohla vyhnout povinnosti neuplatnit zásady „bezpečného přístavu“, která vyplývá z právních norem, jež musí použít.

183. Jsem tedy názoru, že rozhodnutí 2000/520 musí být prohlášeno za neplatné v rozsahu, v němž existence výjimky, jež natolik obecně a nepřesně umožňuje vyloučit použití zásad režimu „bezpečného přístavu“, brání sama o sobě závěru, že tento režim zajišťuje odpovídající úroveň ochrany osobním údajům, které jsou předávány do Spojených států z Unie.

68 — V tomto ohledu viz rozsudek Digital Rights Ireland a další (C-293/12 a C-594/12, EU:C:2014:238, body 39 a 40).

184. Pokud jde nyní o první kategorii omezení stanovených v příloze I čtvrtém pododstavci písm. a) rozhodnutí 2000/520 z důvodu splnění požadavků bezpečnosti státu, veřejného zájmu nebo prosazování amerických zákonů, pouze první cíl se mi jeví jako dostatečně přesný na to, aby byl považován za cíl obecného zájmu uznávaný Unií ve smyslu čl. 52 odst. 1 Listiny.

185. Nyní je třeba ověřit přiměřenost zjištěného zásahu.

186. V tomto ohledu je třeba připomenout, že „podle ustálené judikatury Soudního dvora zásada proporcionality vyžaduje, aby akty unijních orgánů byly způsobilé k dosažení legitimních cílů sledovaných dotčenou právní úpravou a nepřekračovaly meze toho, co je vhodné a nezbytné k dosažení těchto cílů [69].

187. Pokud jde o soudní přezkum dodržování těchto podmínek, „jedná-li se o zásahy do základních práv, rozsah posuzovací pravomoci unijního zákonodárce může být omezen v závislosti na řadě skutečností, mezi něž patří mimo jiné dotyčná oblast, povaha dotčeného práva zaručeného Listinou, povaha a závažnost zásahu a jeho účel“ [70].

188. Jsem názoru, že rozhodnutí, která Komise přijímá na základě čl. 25 odst. 6 směrnice 95/46, podléhají úplnému přezkumu Soudním dvorem z hlediska přiměřenosti posouzení provedeného Komisí ohledně odpovídající úrovně ochrany, kterou poskytuje třetí země na základě „svých vnitrostátních předpisů nebo mezinárodních závazků“.

189. V této souvislosti je třeba poznamenat, že v rozsudku Digital Rights Ireland a další [71] Soudní dvůr rozhodl, že „s ohledem na významnou úlohu ochrany osobních údajů z hlediska základního práva na respektování soukromého života, jakož i na rozsah a závažnost zásahu do tohoto práva, jejž [předmětná] směrnice představuje, je posuzovací pravomoc unijního zákonodárce omezena, takže přezkum musí být přísný“ [72].

190. Takový zásah musí být způsobilý naplnit cíl sledovaný dotčeným unijním aktem a pro dosažení tohoto cíle nezbytný.

191. V tomto ohledu je třeba podotknout, že „pokud jde o právo na respektování soukromého života, podle ustálené judikatury Soudního dvora ochrana tohoto základního práva […] vyžaduje, aby výjimky z ochrany osobních údajů a její omezení byly činěny v mezích toho, co je naprosto nezbytné“ [73].

192. Soudní dvůr bere při svém přezkumu v úvahu též okolnost, že „ochrana osobních údajů, která vyplývá z výslovné povinnosti stanovené v čl. 8 odst. 1 Listiny, má zvláštní význam pro právo na respektování soukromého života zakotvené v jejím článku 7“ [74].

69 — Rozsudek Digital Rights Ireland a další (C-293/12 a C-594/12, EU:C:2014:238, bod 46 a citovaná judikatura).

70 — Tamtéž (bod 47 a citovaná judikatura).

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

72 — Bod 48.

73 — Rozsudek Digital Rights Ireland a další (C-293/12 a C-594/12, EU:C:2014:238, bod 52 a citovaná judikatura).

74 — Tamtéž (bod 53).

193. Podle Soudního dvora, který v tomto směru odkazuje na judikaturu Evropského soudu pro lidská práva, „dotčená unijní právní úprava musí stanovit jasná a přesná pravidla pro rozsah a použití dotčeného opatření, která stanoví minimální požadavky, aby osoby, jejichž údaje byly uchovány, měly dostatečné záruky umožňující účinně chránit jejich osobní údaje proti riziku zneužití a proti veškerému neoprávněnému přistupování k údajům a jejich protiprávnímu využívání“ [75]. Soudní dvůr uvedl, že „[p]otřeba takových záruk je o to významnější v případě, kdy […] jsou osobní údaje zpracovávány automaticky a existuje značné riziko neoprávněného přistupování k těmto údajům“ [76].

194. Mezi přílohou I čtvrtým pododstavcem písm. a) rozhodnutí 2000/520 a čl. 13 odst. 1 směrnice 95/46 existuje podle mého názoru určitá analogie. V prvně zmíněném ustanovení se uvádí, že dodržování zásad „bezpečného přístavu“ může být omezeno „v rozsahu nezbytném pro splnění požadavků bezpečnosti státu, veřejného zájmu nebo prosazování zákonů Spojených států“. V druhém zmíněném ustanovení je stanoveno, že členské státy mohou přijmout legislativní opatření s cílem omezit rozsah povinností a práv uvedených v čl. 6 odst. 1, v článku 10, v čl. 11 odst. 1 a v článcích 12 a 21 této směrnice, pokud toto omezení představuje opatření nezbytné pro zajištění zejména bezpečnosti státu, obrany, veřejné bezpečnosti, předcházení trestným činům a jejich vyšetřování, odhalování a stíhání.

195. Jak Soudní dvůr uvedl v rozsudku IPI [77], ze znění čl. 13 odst. 1 směrnice 95/46 vyplývá, že členské státy mohou přijmout opatření uvedená v tomto ustanovení pouze tehdy, pokud jsou nezbytná. „Nezbytnost“ opatření tak podmiňuje možnost, kterou uvedený článek dává členským státům [78]. U zpracování osobních údajů v rámci Unie je omezení stanovená v článku 13 této směrnice třeba chápat tak, že jsou redukována na nezbytně nutné pro dosažení sledovaného cíle. Totéž platí podle mého názoru pro omezení zásad „bezpečného přístavu“, jež jsou stanovena v příloze I čtvrtém pododstavci rozhodnutí 2000/520.

196. Je přitom nutno konstatovat, že ne všechny jazykové verze zmiňují kritérium nezbytnosti v textu přílohy I čtvrtém pododstavci písm. a) rozhodnutí 2000/520. Tak je tomu zejména u francouzského znění, které uvádí, že „[d]održování […] zásad může být omezeno […] požadavky týkajícími se bezpečnosti státu, veřejného zájmu nebo prosazování zákonů Spojených států“, kdežto například španělské, německé a anglické znění uvádějí, že zavedená omezení musí být nezbytná pro dosažení uvedených cílů.

197. Skutkové okolnosti uváděné předkládajícím soudem a Komisí v jejích výše zmíněných sděleních ovšem beztak jasně ukazují, že uplatňování těchto omezení se v praxi neredukuje na to, co je nezbytně nutné pro dosažení sledovaných cílů.

198. V této souvislosti je třeba podotknout, že se přístup amerických zpravodajských služeb k předaným osobním údajům globálně vztahuje na všechny osoby a všechny prostředky elektronické komunikace, jakož i na všechny předávané údaje, včetně obsahu komunikací, a to bez jakéhokoli rozlišení, omezení nebo výjimek v závislosti na sledovaném cíli obecného zájmu [79].

199. Přístup amerických zpravodajských služeb k předaným údajům se totiž týká globálně všech osob, které využívají služeb elektronických komunikací, aniž je vyžadováno, aby dotyčné osoby představovaly hrozbu pro bezpečnost státu [80].

75 — Tamtéž (bod 54 a citovaná judikatura).

76 — Tamtéž (bod 55 a citovaná judikatura).

77 — C-473/12, EU:C:2013:715.

78 — Bod 32.

79 — Viz obdobně rozsudek Digital Rights Ireland a další (C-293/12 a C-594/12, EU:C:2014:238, bod 57 a citovaná judikatura).

80 — Tamtéž (body 58 a 59).

200. Takovéto rozsáhlé a necílené sledování je svojí povahou nepřiměřené a představuje neodůvodněný zásah do práv zaručených články 7 a 8 Listiny.

201. Jak ve svém vyjádření správně uvedl Parlament, jelikož není možné, aby unijní normotvůrce nebo členské státy přijali legislativní opatření, která by v rozporu s Listinou stanovila rozsáhlé a necílené sledování, nutně z toho vyplývá, že *a fortiori* nelze mít v žádném případě za to, že třetí země zajišťují odpovídající úroveň ochrany osobních údajů unijních občanů, pokud jejich právní předpisy skutečně dovolují rozsáhlé a necílené sledování a zachycování tohoto druhu údajů.

202. Kromě toho je třeba zdůraznit, že režim „bezpečného přístavu“, jak je vymezen v rozhodnutí 2000/520, neobsahuje záruky k zamezení rozsáhlého a globálního přístupu k předávaným údajům.

203. V této souvislosti je nutno podotknout, že Soudní dvůr v rozsudku Digital Rights Ireland a další [81] zdůraznil význam stanovení „jasn[ých] a přesn[ých] pravidel pro rozsah zásahu do základních práv zakotvených v článcích 7 a 8 Listiny“ [82]. Takový zásah musí být podle Soudního dvora „přesně vymezen ustanoveními umožňujícími zaručit, že je skutečně omezen na nezbytné minimum“ [83]. Soudní dvůr v tomto rozsudku rovněž zdůraznil nezbytnost stanovit „dostatečné záruky k zajištění účinné ochrany [osobních] údajů proti riziku zneužití [a] proti veškerému neoprávněnému přistupování k údajům a jejich protiprávnímu využívání, které vyžaduje článek 8 Listiny“ [84].

204. Je přitom nutné konstatovat, že mechanismy soukromého rozhodčího řízení a FTC nepředstavují z důvodu jejich úlohy omezené na obchodní spory prostředky k napadení přístupu amerických zpravodajských služeb k osobním údajům předávaným z Unie.

205. Příslušnost FTC se vztahuje na nekalé nebo klamavé jednání a praktiky v obchodě, a FTC tudíž není příslušná zasahovat v případě shromažďování a využívání osobních informací pro nekomerční účely [85]. Ohraničená pravomoc FTC omezuje právo fyzických osob na ochranu jejich osobních údajů. FTC nebyla zřízena k tomu, aby zajišťovala – jak je tomu v případě vnitrostátních orgánů dozoru v rámci Unie – ochranu individuálního práva na ochranu soukromí, nýbrž aby zaručila poctivý a spolehlivý obchod pro spotřebitele, což *de facto* omezuje její možnosti zásahu v oblasti ochrany osobních údajů. FTC tedy neplní úlohu srovnatelnou s úlohou vnitrostátních orgánů dozoru ve smyslu článku 28 směrnice 95/46.

206. Unijní občané, jejichž osobní údaje byly předány, se mohou obrátit na zvláštní rozhodčí orgány usazené ve Spojených státech, jako např. TRUSTe a BBBOnline, se žádostmi o upřesnění, zda společnost, jež má k dispozici jejich osobní údaje, porušuje podmínky režimu vlastního osvědčení. Soukromé rozhodčí řízení zajišťované takovými orgány, jako je TRUSTe, se nemůže zabývat porušením práva na ochranu osobních údajů, jichž se dopustily jiné subjekty nebo orgány než společnosti s vlastním osvědčením. Tyto rozhodčí orgány nemají žádnou pravomoc k rozhodování o legalitě činností amerických bezpečnostních agentur.

207. Ani FTC ani soukromé rozhodčí orgány tedy nemají pravomoc dohlížet na případné porušování zásad ochrany osobních údajů ze strany takových veřejných subjektů, jako jsou americké bezpečnostní agentury. Tato pravomoc je však zásadní pro plné zaručení práva na účinnou ochranu těchto údajů. Komise tedy nemohla prostřednictvím přijetí rozhodnutí 2000/520 a zachováním jeho platnosti konstatovat, že u všech osobních údajů předaných do Spojených států bude zajištěna odpovídající ochrana práva přiznaného čl. 8 odst. 3 Listiny, tedy že nezávislý orgán vykonává účinný dohled nad dodržováním požadavků ochrany a bezpečnosti těchto údajů.

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

82 — Bod 65.

83 — Tamtéž.

84 — Tamtéž (bod 66).

85 — V tomto ohledu viz příloha II, FAQ 11 rozhodnutí 2000/520, pod nadpisem „Činnost FTC“, a přílohy III, V a VII tohoto rozhodnutí.

208. Je tudíž třeba konstatovat, že v režimu „bezpečného přístavu“ stanoveném v rozhodnutí 2000/520 neexistuje žádný nezávislý orgán, který by mohl dohlížet na to, zda se uplatňování výjimek ze zásad „bezpečného přístavu“ omezuje na nezbytně nutné. Jak bylo uvedeno výše, takový dohled nezávislého orgánu přitom představuje z hlediska unijního práva zásadní prvek respektování ochrany osob v souvislosti se zpracováním osobních údajů [86].

209. V této souvislosti je třeba zdůraznit úlohu, kterou v systému ochrany osobních údajů platném v Unii zaujímají vnitrostátní orgány dozoru při dohledu nad omezeními stanovenými v článku 13 směrnice 95/46. Podle čl. 28 odst. 4 druhého pododstavce této směrnice se „[n]a orgán dozoru […] může zejména obrátit kdokoli s žádostí o ověření přípustnosti zpracování, pokud se uplatní vnitrostátní předpisy přijaté na základě článku 13 této směrnice“. *Per analogiam* jsem názoru, že zmínka o omezeních uplatňování zásad „bezpečného přístavu“ v příloze I čtvrtém pododstavci rozhodnutí 2000/520 měla být doprovázena zavedením kontrolního mechanismu zajišťovaného nezávislým orgánem specializovaným v oblasti ochrany osobních údajů.

210. Zásah nezávislých orgánů dozoru je totiž ústředním prvkem evropského systému ochrany osobních údajů. Existence takovýchto orgánů byla tedy přirozeně považována od počátku za jednu z nezbytných podmínek ke zjištění odpovídající úrovně ochrany poskytované třetími zeměmi. Jedná se o podmínku k tomu, aby toky údajů z území členských států na území třetích zemí nebyly v souladu s článkem 25 směrnice 95/46 zakázány [87]. Jak je uvedeno v diskusním dokumentu vydaném pracovní skupinou založenou na základě článku 29 uvedené směrnice, v Evropě panuje široká shoda na tom, že „nástroj ‚vnějšího dohledu‘ v podobě nezávislého orgánu představuje nezbytný prvek každého systému, jenž má zajistit dodržování pravidel o ochraně osobních údajů“ [88].

211. Navíc podotýkám, že FISC neposkytuje účinnou soudní ochranu unijním občanům, jejichž osobní údaje jsou předávány do Spojených států. Ochrana před sledováním vládními službami v rámci oddílu 702 zákona z roku 1978 o sledování zahraničních zpravodajských služeb se vztahuje výlučně na americké občany a na cizí státní příslušníky s legálním trvalým pobytem ve Spojených státech. Jak uvedla sama Komise, dohled nad programy Spojených států pro shromažďování zpravodajských informací by se zlepšil posílením úlohy soudu FISC a zavedením opravných prostředků pro fyzické osoby. Tyto mechanismy by mohly snížit míru zpracovávání osobních údajů Evropanů, které nejsou důležité pro účely vnitrostátní bezpečnosti [89].

212. Sama Komise mimoto uvedla, že unijní občané nemají možnost získat přístup k údajům, které se jich týkají, možnost opravy či výmazu údajů nebo možnost správní či soudní nápravy ve vztahu k shromažďování a dalšímu zpracování jejich osobních údajů, k němuž dochází v rámci programů USA pro sledování [90].

213. Konečně je třeba uvést, že americké normy v oblasti ochrany soukromí mohou být uplatňovány na americké občany odlišným způsobem než na cizí státní příslušníky [91].

86 — Viz rozsudek Digital Rights Ireland a další (C-293/12 a C-594/12, EU:C:2014:238, bod 68 a citovaná judikatura).

87 — Viz Poullet, Y., „L’autorité de contrôle: ‘vues’ de Bruxelles“, *Revue française d’administration publique*, č. 89, leden–březen 1999, s. 69, konkrétně s. 71.

88 — Viz s. 7 pracovního dokumentu WP 12 Komise, zmíněného v poznámce pod čarou 56.

89 — Strany 10 a 11 sdělení Komise zmíněného v poznámce pod čarou 2.

90 — Viz bod 7.2, s. 20 sdělení Komise zmíněného v poznámce pod čarou 58.

91 — Viz k této ozázce: Kuner, C., „Foreign Nationals and Data Protection Law: A Transatlantic Analysis“, *Data Protection Anno 2014: How To Restore Trust*? Intersentia, Cambridge, 2014, rok 213, konkrétně s. 216 a násl.

214. Z výše uvedeného vyplývá, že rozhodnutí 2000/520 nestanoví jasná a přesná pravidla pro rozsah zásahu do základních práv zakotvených v článcích 7 a 8 Listiny. Je tedy nutno konstatovat, že toto rozhodnutí a jeho uplatňování představuje velmi rozsáhlý a zvlášť závažný zásah do těchto základních práv, aniž je tento zásah přesně vymezen ustanoveními umožňujícími zaručit, že je skutečně omezen na nezbytné minimum.

215. Komise tedy přijetím rozhodnutí 2000/520 a následně zachováním jeho platnosti překročila meze, které plynou z respektování zásady proporcionality s ohledem na články 7, 8 a čl. 52 odst. 1 Listiny. Navíc je třeba konstatovat, že dochází k neodůvodněnému zásahu do práva unijních občanů na účinnou právní ochranu chráněného článkem 47 listiny.

216. Toto rozhodnutí musí být tudíž prohlášeno za neplatné v rozsahu, v němž z důvodu výše popsaného porušení základních práv nelze mít za to, že režim „bezpečného přístavu“, který toto rozhodnutí zavádí, zajišťuje odpovídající úroveň ochrany osobních údajů předávaných v rámci tohoto režimu z Unie do Spojených států.

217. Vzhledem k tomuto zjištění o porušení základních práv unijních občanů jsem názoru, že Komise měla pozastavit uplatňování rozhodnutí 2000/520.

218. Toto rozhodnutí má neomezenou časovou platnost. Projednávaná věc však svědčí o tom, že odpovídající úroveň ochrany poskytovaná třetí zemí se může postupem času vyvíjet v závislosti na změně skutkových i právních okolností, z nichž uvedené rozhodnutí vycházelo.

219. Podotýkám, že samo rozhodnutí 2000/520 obsahuje ustanovení, na jejichž základě může Komise v závislosti na daných okolnostech toto rozhodnutí upravit.

220. Z bodu 9 odůvodnění tohoto rozhodnutí v tomto ohledu vyplývá, že „[j]e možné, že tzv. ‚bezpečný přístav‘ vytvořený zásadami a FAQ bude nutno případně přezkoumávat na základě zkušeností, s ohledem na vývoj v oblasti ochrany soukromí za situace, kdy technologie neustále usnadňují předávání a zpracování osobních údajů, a na základě zpráv orgánů pověřených jeho prosazováním“.

221. Obdobně čl. 3 odst. 4 uvedeného rozhodnutí uvádí, že „[p]okud informace shromážděné podle odstavců 1, 2 a 3 prokážou, že kterýkoli subjekt pověřený zajištěním toho, aby byly dodržovány zásady prováděné v souladu s FAQ ve Spojených státech, neplní účinně svou úlohu, uvědomí o tom Komise ministerstvo obchodu Spojených států, a bude-li třeba, předloží návrh [...] s cílem zrušit toto rozhodnutí, pozastavit je nebo omezit jeho působnost“.

222. Dále podle čl. 4 odst. 1 rozhodnutí 2000/520 lze toto rozhodnutí „kdykoli upravit s ohledem na zkušenosti s jeho uplatňováním nebo jestliže úroveň ochrany poskytovaná zásadami a FAQ bude převýšena požadavky kladenými právem Spojených států. Komise zhodnotí v každém případě provádění tohoto rozhodnutí na základě dostupných informací tři roky po jeho oznámení členským státům a veškeré významné poznatky sdělí výboru zřízenému článkem 31 směrnice 95/46[…], a zejména sdělí veškeré důkazy, které by mohly mít vliv na hodnocení, prováděné podle článku 1 tohoto rozhodnutí, zda poskytují odpovídající úroveň ochrany ve smyslu článku 25 směrnice 95/46“. Podle čl. 4 odst. 2 rozhodnutí 2000/520 „Komise předloží, je-li to nezbytné, návrhy opatření postupem podle článku 31 směrnice 95/46“.

223. Komise ve svém vyjádření konstatovala, že „je „vysoce pravděpodobné, že přijetí zásad ‚bezpečného přístavu‘ bylo omezeno takovým způsobem, že již nesplňuje striktně vymezené podmínky pro výjimku stanovenou v oblasti bezpečnosti státu“ [92]. Komise v tomto ohledu podotýká, že „[z] předmětných zjištění je patrné nediferencované sledování v rozsáhlé míře, které není slučitelné

92 — Bod 44.

s kritériem nezbytnosti stanoveným v této výjimce ani obecně s právem na ochranu osobních údajů zakotveným v článku 8 Listiny“ [93]. Komise mimoto sama konstatovala, že „[d]osah […] programů sledování spolu s nerovným zacházením ve vztahu k občanům [Unie] vyvolává pochybnosti ohledně úrovně ochrany, kterou systém bezpečného přístavu poskytuje“ [94].

224. Komise navíc na jednání výslovně uznala, že v rozhodnutí 2000/520, jak je v současnosti uplatňováno, neexistuje žádná záruka, že právo unijních občanů na ochranu jejich osobních údajů bude zajištěno. Toto zjištění však podle Komise není s to přivodit neplatnost tohoto rozhodnutí. Komise sice souhlasí s tvrzením, že musí reagovat na nové okolnosti, je však názoru, že přijala vhodná a přiměřená opatření tím, že zahájila jednání se Spojenými státy s cílem reformy režimu „bezpečného přístavu“.

225. Tento názor nesdílím. V mezidobí musí být totiž možné předávání osobních údajů do Spojených států zastavit na podnět vnitrostátních orgánů dozoru nebo v návaznosti na stížnosti podané k těmto orgánům.

226. Kromě toho zastávám názor, že vzhledem k těmto zjištěním měla Komise pozastavit uplatňování rozhodnutí 2000/520. Cíl ochrany osobních údajů, který sledují směrnice 95/46 a článek 8 Listiny, zakládá povinnosti nejen členským státům, ale i unijním orgánům, jak plyne z čl. 51 odst. 1 Listiny.

227. Při posuzování úrovně ochrany poskytované třetí zemí musí Komise zkoumat nejen vnitrostátní právní předpisy a mezinárodní závazky této třetí země, ale též způsob, jakým je ochrana osobních údajů zajišťována v praxi. Vyjdou-li při zkoumání této praxe najevo určité nedostatky, musí Komise reagovat, a případně pozastavit uplatňování svého rozhodnutí nebo jej upravit.

228. Jak bylo uvedeno v předchozích úvahách, povinnost členských států spočívá především v tom, aby prostřednictvím svých vnitrostátních orgánů dozoru zajistily dodržování pravidel stanovených ve směrnici 95/46.

229. Povinností Komise je pozastavit uplatňování rozhodnutí, které přijala na základě čl. 25 odst. 6 této směrnice v případě prokázaného neplnění povinností ze strany dotyčné třetí země, po dobu jednání, které Komise vede s touto třetí zemí s cílem ustat v tomto neplnění.

230. Připomínám, že účelem rozhodnutí přijatého Komisí na základě tohoto ustanovení je konstatovat, že třetí země „zajišťuje“ odpovídající úroveň ochrany osobních údajů, které jsou do této třetí země předávány. Výraz „zajišťuje“ v přítomném čase znamená, že aby platnost tohoto rozhodnutí mohla být zachována, musí se týkat třetí země, která i po přijetí uvedeného rozhodnutí nadále zaručuje odpovídající úroveň ochrany.

231. V bodě 57 odůvodnění směrnice 95/46 se uvádí, že „v případě, kdy třetí země […] neposkytuje odpovídající úroveň ochrany, musí být předávání osobních údajů do této země zakázáno“.

232. Podle čl. 25 odst. 4 této směrnice, „[p]okud Komise zjistí, postupem podle čl. 31 odst. 2, že třetí země nezajišťuje odpovídající úroveň ochrany ve smyslu odstavce 2 tohoto článku, přijmou členské státy opatření nezbytná pro zamezení jakémukoli předávání údajů stejného druhu do dotčené třetí země“. Kromě toho čl. 25 odst. 5 uvedené směrnice stanoví, že „[v]e vhodný okamžik Komise zahájí jednání s cílem napravit stav vyplývající ze zjištění podle odstavce 4“.

93 — Tamtéž.

94 — Viz s. 5 sdělení Komise zmíněného v poznámce pod čarou 2.

233. Z posledně zmíněného ustanovení vyplývá, že v systému zavedeném článkem 25 směrnice 95/46 mají jednání započatá se třetí zemí za cíl napravit nedostatek odpovídající úrovně ochrany zjištěný postupem podle čl. 31 odst. 2 této směrnice. V projednávaném případě Komise v souladu s tímto postupem formálně nekonstatovala, že by režim „bezpečného přístavu“ již nezajišťoval odpovídající úroveň ochrany. Pokud se však Komise rozhodla zahájit jednání se Spojenými státy, učinila tak proto, že byla názoru, že úroveň ochrany zajišťované touto třetí zemí již není odpovídající.

234. Ačkoli Komise věděla o nedostatcích v uplatňování rozhodnutí 2000/520, nepozastavila toto rozhodnutí ani jej nijak neupravila, což vedlo k tomu, že nadále jsou porušována základní práva osob, jejichž osobní údaje byly a stále jsou předávány v rámci režimu „bezpečného přístavu“.

235. Soudní dvůr přitom již rozhodl – byť v jiném kontextu – že Komise musí dbát na přizpůsobení právní úpravy novým údajům [95].

236. Takováto nečinnost Komise, která přímo zasahuje do základních práv chráněných články 7, 8 a 47 Listiny, představuje podle mého názoru další důvod k tomu, aby rozhodnutí 2000/520 bylo v rámci tohoto řízení o předběžné otázce prohlášeno za neplatné [96].

## III – **Závěry**

237. Vzhledem k výše uvedeným úvahám navrhuji Soudnímu dvoru, aby na otázky položené High Court odpověděl následovně:

„Článek 28 směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů, ve spojení s články 7 a 8 Listiny základních práv Evropské unie, musí být vykládán v tom smyslu, že existence rozhodnutí přijatého Evropskou komisí na základě čl. 25 odst. 6 směrnice 95/46 nebrání vnitrostátnímu orgánu dozoru v prošetření stížnosti, v níž se tvrdí, že třetí země nezajišťuje odpovídající úroveň ochrany předávaných osobních údajů, a případně v zastavení předávání těchto údajů.

Rozhodnutí Komise 2000/520/ES ze dne 26. července 2000 podle směrnice Evropského parlamentu a Rady 95/46/ES o odpovídající ochraně poskytované podle zásad ‚bezpečného přístavu‘, a s tím souvisejících ‚často kladených otázek‘ vydaných ministerstvem obchodu Spojených států je neplatné.“

95 — V tomto smyslu viz rozsudek Agrarproduktion Staebelow (C-504/04, EU:C:2006:30, bod 40).

96 — Ačkoli Soudní dvůr v rozsudku T. Port (C-68/95, EU:C:1996:452) rozhodl, že „Smlouva nestanovila možnost podat žádost o rozhodnutí o předběžné otázce, v níž by vnitrostátní soud žádal Soudní dvůr, aby v rámci řízení o předběžné otázce určil nečinnost daného orgánu“ (bod 53), zdá se, že vůči této možnosti zaujal kladnější postoj v rozsudku Ten Kate Holding Musselkanaal a další (C-511/03, EU:C:2005:625, bod 29).