



Sbírka soudních rozhodnutí

STANOVISKO GENERÁLNÍHO ADVOKÁTA
HENRIKA SAUGMANDSGAARDA ØE
přednesené dne 19. prosince 2019¹

Věc C-311/18

**Data Protection Commissioner
proti
Facebook Ireland Limited,
Maximillianu Schremsovi,
za účasti
Spojených států amerických,
Electronic Privacy Information Centre,
BSA Business Software Alliance, Inc.,
Digitaleurope**

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

„Řízení o předběžné otázce – Ochrana fyzických osob v souvislosti se zpracováním osobních údajů – Nařízení (EU) č. 2016/679 – Článek 2 odst. 2 – Působnost – Předávání osobních údajů pro obchodní účely do Spojených států amerických – Zpracování předaných údajů orgány veřejné moci Spojených států amerických pro účely národní bezpečnosti – Článek 45 – Posouzení odpovídající úrovně ochrany zajišťované třetí zemí – Článek 46 – Vhodné záruky poskytnuté správcem – Standardní doložky o ochraně – Článek 58 odst. 2 – Pravomoci orgánů dozoru – Rozhodnutí 2010/87/EU – Platnost – Prováděcí rozhodnutí (EU) 2016/1250 – „Štít EU-USA na ochranu soukromí“ – Platnost – Články 7, 8 a 47 Listiny základních práv Evropské unie“

Obsah

I. Úvod	3
II. Právní rámec	4
A. Směrnice 95/46/ES	4
B. GDPR	6
C. Rozhodnutí 2010/87	10
D. Rozhodnutí o štítu na ochranu soukromí	14

¹ – Původní jazyk: francouzština.

III. Spor v původním řízení, předběžné otázky a řízení před Soudním dvorem	15
IV. Analýza	23
A. Úvodní poznámky	23
B. K přípustnosti žádosti o rozhodnutí o předběžné otázce	24
1. K časové působnosti směrnice 95/46	25
2. K předběžné povaze pochybností vyjádřených DPC	26
3. K nejistotě ohledně vymezení skutkového rámce	26
C. K použitelnosti unijního práva na předávání osobních údajů za obchodními účely do třetího státu, který je může zpracovávat pro účely národní bezpečnosti (první otázka)	27
D. K úrovni ochrany vyžadované v rámci předávání založeného na standardních smluvních doložkách (první část šesté otázky)	28
E. K platnosti rozhodnutí 2010/87 s ohledem na články 7, 8 a 47 Listiny (sedmá, osmá a jedenáctá otázka)	30
1. K povinnostem správců	31
2. K povinnostem orgánů dozoru	33
F. K neexistenci nutnosti odpovědět na ostatní předběžné otázky a přezkoumat platnost rozhodnutí o štítu na ochranu soukromí	36
1. K neexistenci nutnosti odpovědi Soudního dvora s ohledem na předmět sporu v původním řízení	36
2. K důvodům, které svědčí v neprospěch přezkumu Soudního dvora s ohledem na předmět řízení probíhajícího u DPC	38
G. Podpůrné poznámky týkající se účinků a platnosti rozhodnutí o štítu na ochranu soukromí	40
1. K dopadu rozhodnutí o štítu na ochranu soukromí v rámci vyřízení stížnosti týkající se legality předávání na základě smluvních záruk orgánem dozoru	40
2. K platnosti rozhodnutí o štítu na ochranu soukromí	41
a) Upřesnění týkající se obsahu přezkumu platnosti rozhodnutí o odpovídající úrovni ochrany	42
1) K obsahu srovnání, které umožňuje posoudit „podstatnou rovnocennost“ úrovně ochrany	42
2) K nezbytnosti zajistit odpovídající úroveň ochrany během předávání údajů	47
3) K zohlednění skutkových zjištění provedených Komisí a předkládajícím soudem ohledně práva Spojených států	48
4) K dosahu standardu „podstatné rovnocennosti“	49

b) K platnosti rozhodnutí o štítu na ochranu soukromí z hlediska práv na respektování soukromého života a ochrany osobních údajů	51
1) K existenci zásahů	51
2) K povaze zásahů „stanovených zákonem“	52
3) K neexistenci zásahu do podstaty základních práv	54
4) Ke sledování oprávněného cíle	57
5) K nezbytnosti a přiměřenosti zásahů	58
c) K platnosti rozhodnutí o štítu na ochranu soukromí s ohledem na právo na účinnou právní ochranu	61
1) K účinnosti právem USA stanovených prostředků nápravy před soudem	62
2) K dopadu mechanismu ombudsmana na úroveň ochrany práva na účinnou právní ochranu	65
V. Závěry	67

I. Úvod

1. Vzhledem k neexistenci společných záruk v oblasti ochrany osobních údajů na světové úrovni jsou přeshraniční toky takových údajů spojeny s rizikem přerušení kontinuity úrovně ochrany zajištěné v rámci Evropské unie. Za účelem usnadnění těchto toků při současném omezení tohoto rizika unijní normotvůrce zavedl tři mechanismy, na základě kterých mohou být osobní údaje předávány z Unie do třetího státu.

2. Zaprvé takové předání lze provést na základě rozhodnutí, v němž Evropská komise konstatuje, že dotčený třetí stát zajišťuje „odpovídající úroveň ochrany“ údajů, které jsou do něj předávány². Zadruhé v případě neexistence takového rozhodnutí je předání povoleno tehdy, pokud je spojeno s „vhodnými zárukami“³. Tyto záruky mohou mít podobu smlouvy mezi vývozcem a dovozcem údajů, která obsahuje standardní doložky o ochraně přijaté Komisí. GDPR stanoví zatřetí určité výjimky, založené zejména na souhlasu dotčené osoby, umožňující předání do třetí země i v případě, že neexistuje rozhodnutí o odpovídající ochraně ani vhodné záruky⁴.

3. Žádost o rozhodnutí o předběžné otázce podaná High Court (Vrchní soud, Irsko) se týká druhého z těchto mechanismů. Konkrétně se týká platnosti rozhodnutí 2010/87/EU⁵, kterým Komise stanovila standardní smluvní doložky pro některé kategorie předávání s ohledem na články 7, 8 a 47 Listiny základních práv Evropské unie (dále jen „Listina“).

2 – Viz článek 45 nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46 (obecné nařízení o ochraně osobních údajů) (Úř. věst. 2016, L 119, s. 1, dále jen „GDPR“).

3 – Viz článek 46 GDPR.

4 – Viz článek 49 GDPR.

5 – Rozhodnutí Komise ze dne 5. února 2010 o standardních smluvních doložkách pro předávání osobních údajů zpracovatelům usazeným ve třetích zemích podle směrnice Evropského parlamentu a Rady 95/46/ES (Úř. věst. 2010, L 39, s. 5) ve znění prováděcího rozhodnutí Komise (EU) 2016/2297 ze dne 16. prosince 2016 (Úř. věst. 2016, L 344, s. 100) (dále jen „rozhodnutí 2010/87“).

4. Tato žádost byla podána v rámci sporu mezi Data Protection Commissioner (komisař pro ochranu údajů, Irsko, dále jen „DPC“) na straně jedné a společností Facebook Ireland Ltd a Maximillianem Schremsem na straně druhé. M. Schrems podal k DPC stížnost týkající se předávání osobních údajů, které se ho týkají, společností Facebook Ireland společnosti Facebook Inc., která je její mateřskou společností se sídlem ve Spojených státech amerických (dále jen „Spojené státy“). DPC má za to, že vyřízení této stížnosti závisí na tom, zda je rozhodnutí 2010/87 platné. V tomto kontextu se DPC obrátil na předkládací soud a požádal jej, aby se v tomto ohledu dotázal Soudního dvora.

5. Předdesílám, že přezkum předběžných otázek podle mého názoru neodhalil žádnou skutečnost, kterou by mohla být platnost rozhodnutí 2010/87 dotčena.

6. Předkládající soud kromě toho uvedl určité pochybnosti, které se v podstatě týkají odpovídající úrovně ochrany zajišťované Spojenými státy s ohledem na zásahy do výkonu základních práv osob, jejichž údaje jsou předávány do této třetí země, z důvodu činností amerických zpravodajských orgánů. Tyto pochybnosti nepřímo zpochybňují posouzení provedené Komisí v tomto ohledu v prováděcím rozhodnutí (EU) 2016/1250⁶. I když řešení sporu v původním řízení nevyžaduje, aby Soudní dvůr tuto otázku rozhodl, a v důsledku toho navrhuji, aby Soudní dvůr na tuto otázku neodpovídal, uvedu podpůrně důvody, které mě vedou k tomu, že se budu zabývat platností tohoto rozhodnutí.

7. Celá moje analýza bude vedena snahou o rovnováhu jednak mezi nutností prokázat „rozumný stupeň pragmatismu s cílem umožnit interakci se zbytkem světa“⁷ a jednak nezbytností potvrdit základní hodnoty uznané v právních řádech Unie a jejích členských států, zejména Listinou.

II. Právní rámec

A. Směrnice 95/46/ES

8. Článek 3 odst. 2 směrnice 95/46/ES o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů⁸ stanovoval:

„Tato směrnice se nevztahuje na zpracování osobních údajů:

- prováděné pro výkon činností, které nespádají do oblasti působnosti práva Společenství a jsou uvedeny [které nespádají do oblasti působnosti práva Společenství, jako jsou činnosti uvedené] v hlavě V a VI Smlouvy o Evropské unii, a v každém případě na zpracování, které se týká veřejné bezpečnosti, obrany, bezpečnosti státu (včetně hospodářské stability státu, pokud jsou tato zpracování spojená s otázkami bezpečnosti státu) a činnosti státu v oblasti trestního práva,

[...]“

6 – Rozhodnutí Komise ze dne 12. července 2016 podle [směrnice 95/46] o odpovídající úrovni ochrany poskytované štítem EU–USA na ochranu soukromí (Úř. věst. 2016, L 207, s. 1, dále jen „rozhodnutí o štítu na ochranu soukromí“).

7 – Viz pojednání bývalého evropského inspektora ochrany údajů (ESOOÚ) P. Hustinx, „Le droit de l'Union européenne sur la protection des données: la révision de la directive 95/46/CE et la proposition de règlement général sur la protection des données“, s. 49, dostupné na adrese https://edps.europa.eu/sites/edp/files/publication/14-09-15_article_eui_fr.pdf.

8 – Směrnice Evropského parlamentu a Rady ze dne 24. října 1995 (Úř. věst. 1995, L 281, s. 31; Zvl. vyd. 13/15, s. 355) ve znění nařízení Evropského parlamentu a Rady (ES) č. 1882/2003 ze dne 29. září 2003 (Úř. věst. 2003, L 284, s. 1; Zvl. vyd. 01/004, s. 447) (dále jen „směrnice 95/46“).

9. Článek 13 odst. 1 této směrnice zněl takto:

„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 člancích 12 a 21, pokud toto omezení představuje opatření nezbytné pro zajištění:

- a) bezpečnosti státu;
- b) obrany;
- c) veřejné bezpečnosti;
- d) předcházení trestným činům a jejich vyšetřování, odhalování a stíhání nebo nedodržování deontologických pravidel pro regulovaná povolání;
- e) významného hospodářského nebo finančního zájmu členského státu nebo [Unie], včetně měnové, rozpočtové a daňové oblasti;
- f) kontrolní, inspekční nebo regulační funkce vyplývající, i pouze příležitostně, z výkonu veřejné moci v případech uvedených v písmenech c), d) a e);
- g) ochrany subjektu údajů nebo práv a svobod druhých.“

10. Článek 25 uvedené směrnice uváděl:

„1. Členské státy stanoví, 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 této směrnice, pouze pokud dotyčná třetí země zajistí odpovídající úroveň ochrany.

2. Odpovídající 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.

[...]

6. 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 svých mezinárodních závazků sjednaných zejména na závěr jednání uvedených v odstavci 5 s cílem zajistit ochranu soukromí a základních práv a svobod osob.

Členské státy přijmou opatření nezbytná pro dosažení souladu s rozhodnutím Komise.“

11. Článek 26 odst. 2 a 4 téže směrnice stanovoval:

„2. Aniž je tím dotčen odstavec 1, může členský stát povolit předání nebo předávání osobních údajů do třetí země, která nezajišťuje odpovídající úroveň ochrany ve smyslu čl. 25 odst. 2, pokud správce poskytne dostatečná ochranná opatření [dostatečné záruky] pro ochranu soukromí a základních práv a svobod osob, jakož i pro výkon odpovídajících práv; tato ochranná opatření [tyto záruky] mohou zejména vyplývat z vhodných smluvních doložek.

[...]

4. Pokud Komise rozhodne [...], že některé standardní smluvní doložky představují dostatečná ochranná opatření uvedená [dostatečné záruky uvedené] v odstavci 2, přijmou členské státy opatření nezbytná pro dosažení souladu s rozhodnutím Komise.“

12. Článek 28 odst. 3 směrnice 95/46 zněl takto:

„Každý orgán dozoru má zejména:

[...]

- pravomoci účinně zasáhnout, jako například zaujmout stanovisko před zahájením zpracování v souladu s článkem 20 a zajistit vhodné zveřejnění těchto stanovisek nebo pravomoc nařídit blokování, výmaz nebo zničení údajů nebo dočasně nebo trvale zakázat zpracování nebo pravomoc zaslat správci upozornění či napomenutí nebo pravomoc obrátit se na parlament členského státu či na jiné politické orgány;
- [...]“

B. GDPR

13. Na základě čl. 94 odst. 1 GDPR toto nařízení zrušilo směrnicí 95/46 s účinností k 25. květnu 2018, což je datum, ke kterému se toto nařízení začalo používat v souladu s jeho čl. 99 odst. 2.

14. Článek 2 odst. 2 uvedeného nařízení stanoví:

„Toto nařízení se nevztahuje na zpracování osobních údajů prováděné:

- a) při výkonu činností, které nespádají do oblasti působnosti práva Unie;
- b) členskými státy při výkonu činností, které spadají do oblasti působnosti hlavy V kapitoly 2 Smlouvy o EU;

[...]

- d) příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, včetně ochrany před hrozbami pro veřejnou bezpečnost a jejich předcházení.“

15. Článek 4 bod 2 téhož nařízení vymezuje „zpracování“ jako „jakoukoli operaci nebo soubor operací s osobními údaji nebo soubory osobních údajů, který je prováděn pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení“.

16. Článek 23 GDPR stanoví:

„1. Právo Unie nebo členského státu, které se na správce nebo zpracovatele vztahuje, může prostřednictvím legislativního opatření omezit rozsah povinností a práv uvedených v člácích 12 až 22 a v článku 34, jakož i v článku 5, v rozsahu, v jakém ustanovení tohoto článku odpovídají právům a povinnostem stanoveným v člácích 12 až 22, jestliže takové omezení respektuje podstatu základních práv a svobod a představuje nezbytné a přiměřené opatření v demokratické společnosti s cílem zajistit:

- a) národní bezpečnost;

- b) [národní] obranu;
- c) veřejnou bezpečnost;
- d) prevenci, vyšetřování, odhalování či stíhání trestných činů nebo výkon trestů, včetně ochrany před hrozbami pro veřejnou bezpečnost a jejich předcházení;
- e) jiné důležité cíle obecného veřejného zájmu Unie nebo členského státu, zejména důležitý hospodářský nebo finanční zájem Unie nebo členského státu [...];

[...]

2. Každé legislativní opatření uvedené v odstavci 1 zejména obsahuje konkrétní ustanovení, alespoň, je-li to relevantní, pokud jde o:

- a) účely zpracování nebo kategorie zpracování;
- b) kategorie osobních údajů;
- c) rozsah zavedených omezení;
- d) záruky proti zneužití údajů nebo protiprávnímu přístupu k nim či jejich protiprávnímu předání;
- e) specifikaci správců nebo kategorie správců;
- f) doby uložení a platné záruky s ohledem na povahu, rozsah a účely zpracování nebo kategorie zpracování;
- g) rizika z hlediska práv a svobod subjektů údajů; a
- h) právo subjektů údajů být informováni o daném omezení, pokud toto informování nemůže být na újmu účelu omezení.“

17. Článek 44 tohoto nařízení, nadepsaný „Obecná zásada pro předávání“, stanoví:

„K jakémukoli předání osobních údajů, které jsou předmětem zpracování nebo které jsou určeny ke zpracování po předání do třetí země nebo mezinárodní organizaci, může dojít pouze tehdy, splní-li správce a zpracovatel v závislosti na dalších ustanoveních tohoto nařízení podmínky stanovené v této kapitole, včetně podmínek pro další předávání osobních údajů z dané třetí země nebo mezinárodní organizace do jiné třetí země nebo jiné mezinárodní organizaci. Veškerá ustanovení této kapitoly se použijí s cílem zajistit, aby úroveň ochrany fyzických osob zaručená tímto nařízením nebyla znehodnocena.“

18. V souladu s článkem 45 uvedeného nařízení, nadepsaným „Předání založené na rozhodnutí o odpovídající ochraně“, platí:

„1. Předávání osobních údajů do určité třetí země nebo určité mezinárodní organizaci se může uskutečnit, jestliže Komise rozhodla, že tato třetí země, určité území nebo jedno či více konkrétních odvětví v této třetí zemi nebo tato mezinárodní organizace zajišťují odpovídající úroveň ochrany. Takovéto předání nevyžaduje žádné zvláštní povolení.

2. Při posuzování odpovídající úrovně ochrany vezme Komise v úvahu zejména tyto prvky:

- a) právní stát, dodržování lidských práv a základních svobod, příslušné právní předpisy, obecné i odvětvové, včetně těch, které se týkají veřejné bezpečnosti, obrany, národní bezpečnosti a trestního práva a přístupu orgánů veřejné moci k osobním údajům, jakož i provádění těchto právních předpisů, pravidla ochrany údajů, profesní pravidla a související bezpečnostní opatření, včetně pravidel dalšího předávání osobních údajů do další třetí země nebo mezinárodní organizaci, která jsou v dané třetí zemi nebo mezinárodní organizaci dodržována, judikaturu, jakož i existenci účinných a vymahatelných práv subjektu údajů a účinné správní a soudní ochrany pro subjekty údajů, jejichž osobní údaje se předávají;
- b) existenci a účinné fungování jednoho nebo více nezávislých dozorových úřadů, které působí v dané třetí zemi nebo kterým podléhá daná mezinárodní organizace, příslušných zajišťovat a vymáhat souladu s pravidly pro ochranu údajů, včetně přiměřených vymáhacích pravomocí, poskytovat pomoc a poradenství subjektům údajů při výkonu jejich práv a spolupracovat s dozorovými úřady členských států, a
- c) mezinárodní závazky, které daná třetí země nebo mezinárodní organizace přijala, nebo jiné závazky vyplývající z právně závazných úmluv nebo nástrojů, jakož i z její účasti v mnohostranných či regionálních systémech, zejména pokud jde o ochranu osobních údajů.

3. Komise může po posouzení odpovídající úrovně ochrany prostřednictvím prováděcího aktu rozhodnout, že určitá třetí země, určité území či jedno nebo více konkrétních odvětví v určité třetí zemi nebo určitá mezinárodní organizace zajišťuje odpovídající úroveň ochrany ve smyslu odstavce 2 tohoto článku. Uvedený prováděcí akt stanoví mechanismus pro pravidelný přezkum prováděný nejméně každé čtyři roky, který zohlední veškerý relevantní vývoj v dotčené třetí zemi nebo mezinárodní organizaci. [...]

4. Komise průběžně sleduje vývoj ve třetích zemích a mezinárodních organizacích, jenž by mohl ovlivnit fungování rozhodnutí přijatých podle odstavce 3 tohoto článku a rozhodnutí přijatých na základě čl. 25 odst. 6 [směrnice 95/46].

5. Komise v případě, že to vyplývá z dostupných informací, zejména na základě přezkumu uvedeného v odstavci 3 tohoto článku, rozhodne, že určitá třetí země, určité území nebo konkrétní odvětví v určité třetí zemi nebo určitá mezinárodní organizace již nezajišťuje odpovídající úroveň ochrany ve smyslu odstavce 2 tohoto článku, [V případě, že z dostupných informací, zejména na základě přezkumu uvedeného v odstavci 3 tohoto článku, vyplývá, že určitá třetí země, určité území nebo konkrétní odvětví v určité třetí zemi nebo určitá mezinárodní organizace již nezajišťuje odpovídající úroveň ochrany ve smyslu odstavce 2 tohoto článku, Komise] v nezbytné míře rozhodnutí uvedené v odstavci 3 tohoto článku prováděcími akty bez zpětné působnosti zruší nebo změní anebo pozastaví jeho použitelnost. [...]

6. Komise zahájí s danou třetí zemí nebo mezinárodní organizací konzultace s cílem napravit stav, který vedl k rozhodnutí podle odstavce 5.

[...]

9. Rozhodnutí přijatá Komisí na základě čl. 25 odst. 6 [směrnice 95/46] zůstávají platná až do chvíle, kdy je Komise změní, nahradí nebo zruší rozhodnutím přijatým podle odstavce 3 nebo 5 tohoto článku.“

19. Článek 46 téhož nařízení, nadepsaný „Předávání založené na vhodných zárukách“, stanoví následující:

„1. Jestliže neexistuje rozhodnutí podle čl. 45 odst. 3, správce nebo zpracovatel mohou předat osobní údaje do třetí země nebo mezinárodní organizaci, pouze pokud správce nebo zpracovatel poskytl vhodné záruky a za podmínky, že jsou k dispozici vymahatelná práva subjektu údajů a účinná právní ochrana subjektů údajů.

2. Vhodné záruky uvedené v odstavci 1 mohou být stanoveny, aniž je zapotřebí jakékoli zvláštní povolení dozorového úřadu, pomocí:

[...]

c) standardních doložek o ochraně osobních údajů přijatých Komisí přezkumným postupem podle čl. 93 odst. 2;

[...]

5. Povolení členského státu nebo dozorového úřadu na základě čl. 26 odst. 2 [směrnice 95/46] zůstávají platná až do chvíle, kdy je dozorový úřad v případě potřeby změny, nahradí nebo zruší. Rozhodnutí přijatá Komisí na základě čl. 26 odst. 4 [směrnice 95/46] zůstávají platná až do chvíle, kdy je Komise podle potřeby změny, nahradí nebo zruší rozhodnutím přijatým podle odstavce 2 tohoto článku.“

20. Podle článku 58 odst. 2, 4 a 5 GDPR platí:

„2. Každý dozorový úřad má všechny tyto nápravné pravomoci:

- a) upozornit správce či zpracovatele, že zamýšlené operace zpracování pravděpodobně porušují toto nařízení;
- b) udělit napomenutí správci či zpracovateli, jehož operace zpracování porušily toto nařízení;
- c) nařídit správci nebo zpracovateli, aby vyhověli žádostem subjektu údajů o výkon jeho práv podle tohoto nařízení;
- d) nařídit správci či zpracovateli, aby uvedl operace zpracování do souladu s tímto nařízením, a to případně předepsaným způsobem a ve stanovené lhůtě;
- e) nařídit správci, aby subjektu údajů oznámil případy porušení zabezpečení osobních údajů;
- f) uložit dočasné nebo trvalé omezení zpracování, včetně jeho zákazu;

[...]

- i) uložit správní pokutu podle článku 83 vedle či namísto opatření uvedených v tomto odstavci, podle okolností každého jednotlivého případu;
- j) nařídit přerušování toků údajů příjemci ve třetí zemi nebo toků údajů mezinárodní organizaci.

[...]

4. Výkon pravomocí svěřených tímto článkem dozorovému úřadu podléhá vhodným zárukám, včetně účinné soudní ochrany a spravedlivého procesu, stanoveným v právu Unie a členského státu v souladu s Listinou.

5. Každý členský stát v právních předpisech stanoví, že jeho dozorový úřad má pravomoc upozornit na porušení tohoto nařízení justiční orgány, a pokud je to vhodné, zahájit soudní řízení či se do něj jinak zapojit s cílem vymoci dodržení tohoto nařízení.“

C. Rozhodnutí 2010/87

21. Článek 26 odst. 4 směrnice 95/46 vedl ke třem rozhodnutím Komise, ve kterých Komise konstatovala, že standardní smluvní doložky uvedené v těchto rozhodnutích poskytují dostatečné záruky s ohledem na ochranu soukromí a základních práv a svobod jednotlivců, jakož i s ohledem na výkon odpovídajících práv (dále jen „rozhodnutí SSD“)⁹.

22. Mezi těmito rozhodnutími je i rozhodnutí 2010/87, jehož článek 1 stanoví, že „[s]tandardní smluvní doložky uvedené v příloze jsou považovány za dostatečná ochranná opatření [dostatečné záruky] s ohledem na ochranu soukromí a základních práv a svobod jednotlivců, jakož i s ohledem na výkon odpovídajících práv v souladu s čl. 26 odst. 2 [směrnice 95/46]“.

23. Podle článku 3 tohoto rozhodnutí platí:

„Pro účely tohoto rozhodnutí se:

[...]

c) ‚vývozcem údajů‘ rozumí správce, který předává osobní údaje;

d) ‚dovozcem údajů‘ rozumí zpracovatel usazený ve třetí zemi, který se zavazuje přijímat od vývozce údaje osobní údaje určené ke zpracování jménem vývozce údajů po předání v souladu s jeho pokyny a s podmínkami tohoto rozhodnutí a který nepodléhá systému třetí země zajišťující odpovídající ochranu ve smyslu čl. 25 odst. 1 [směrnice 95/46];

[...]

f) ‚právem rozhodným pro ochranu údajů‘ rozumí právní předpisy ochraňující základní práva a svobody jednotlivců, a zejména jejich právo na soukromí ve vztahu ke zpracování osobních údajů, které se vztahují na správce údajů v členském státě, ve kterém je usazen vývozce údajů;

[...]“

⁹ – Rozhodnutí Komise 2001/497/ES ze dne 15. června 2001 o standardních smluvních doložkách pro předávání osobních údajů do třetích zemí podle směrnice [95/46] (Úř. věst. 2001, L 181, s. 19; Zvl. 13/26, s. 347); rozhodnutí Komise 2004/915/ES ze dne 27. prosince 2004, kterým se mění rozhodnutí [2001/497], pokud jde o zavedení alternativního souboru standardních smluvních doložek pro předávání osobních údajů do třetích zemí (Úř. věst. 2004, L 385, s. 74), jakož i rozhodnutí 2010/87.

24. V původním znění článek 4 uvedeného rozhodnutí v odstavci 1 stanovoval:

„Aniž jsou dotčeny jejich pravomoci přijmout opatření k zajištění dodržování vnitrostátních předpisů přijatých podle kapitol II, III, V a VI směrnice 95/46[...], mohou příslušné orgány členských států vykonávat své stávající pravomoci zakázat nebo pozastavit toky údajů směřující do třetích zemí, aby tak chránily jednotlivce v souvislosti se zpracováním jejich osobních údajů v případech, kdy:

- a) je zjištěno, že právní předpisy, kterým dovozce údajů nebo dílčí zpracovatel podléhá, po něm vyžadují, aby se odchýlil od práva rozhodného pro ochranu údajů v rozsahu překračujícím omezení nezbytná v demokratické společnosti, jak je stanoveno v článku 13 směrnice 95/46[...], pokud tyto požadavky mají pravděpodobně výrazně nepříznivý dopad na záruky poskytované právem rozhodným pro ochranu údajů a standardními smluvními doložkami;
- b) příslušný orgán zjistil, že dovozce údajů nebo dílčí zpracovatel nedodržel standardní smluvní doložky uvedené v příloze nebo
- c) je vysoce pravděpodobné, že standardní smluvní doložky uvedené v příloze nejsou nebo nebudou dodržovány a pokračující předávání by pro subjekt údajů představovalo bezprostřední riziko vzniku značné újmy.“

25. Článek 4 rozhodnutí 2010/87 ve stávajícím znění, které vyplývá ze změny rozhodnutí 2010/87 prováděcím rozhodnutím (EU) 2016/2297¹⁰, stanoví, že „[p]okud příslušné orgány v členských státech uplatní pravomoc podle čl. 28 odst. 3 směrnice 95/46[...] a to povede k dočasnému nebo trvalému zákazu toku údajů do třetích zemí za účelem ochrany fyzických osob s ohledem na zpracování jejich osobních údajů, oznámí dotčený členský stát tuto skutečnost bezodkladně Komisi, která tyto informace předá ostatním členským státům“.

26. Příloha rozhodnutí 2010/87 obsahuje soubor standardních smluvních doložek. Konkrétně doložka 3 obsažená v této příloze, nadepsaná „Doložka ve prospěch třetí strany“, stanoví:

„1. Subjekty údajů mohou vůči vývozci údajů uplatnit jako oprávněné třetí strany tuto doložku, doložku 4 písm. b) až i), doložku 5 písm. a) až e) a g) až j), doložku 6 odst. 1 a 2, doložku 7, doložku 8 odst. 2 a doložky 9 až 12.

2. Subjekty údajů mohou vůči dovozci údajů uplatnit tuto doložku, doložku 5 písm. a) až e) a g), doložku 6, doložku 7, doložku 8 odst. 2 a doložky 9 až 12 v případech, kdy vývozce údajů fakticky zmizel nebo kdy z právního hlediska zanikl, ledaže případný nástupnický subjekt převzal na základě smlouvy nebo právních předpisů veškeré právní povinnosti vývozce údajů a v důsledku toho přijímá práva a povinnosti vývozce údajů, přičemž v tomto případě je subjekt údajů může uplatňovat vůči tomuto subjektu.

[...]“

27. Doložka 4 stanovená v uvedené příloze, nadepsaná „Povinnosti vývozce údajů“, stanoví:

„Vývozce údajů se zavazuje a zaručuje, že:

- a) zpracování osobních údajů, včetně předávání samotného, bylo a bude i nadále prováděno v souladu se souvisejícími ustanoveními práva rozhodného pro ochranu údajů (a případně bylo oznámeno příslušným orgánům členského státu, ve kterém je vývozce údajů usazen) a že neporušuje související předpisy daného státu;

10 – Rozhodnutí Komise ze dne 16. prosince 2016, kterým se mění rozhodnutí [2001/497] a [2010/87] o standardních smluvních doložkách pro předávání osobních údajů do třetích zemí a zpracovatelům usazeným v těchto zemích podle směrnice [95/46] (Úř. věst. 2016, L 344, s. 100).

- b) nařídil a po celou dobu poskytování služeb zpracování osobních údajů bude dovozci údajů nařizovat, aby předávané osobní údaje byly zpracovávány pouze jménem vývozce údajů a v souladu s právem rozhodným pro ochranu údajů a s doložkami;
- c) dovozce údajů poskytne dostatečné záruky v souvislosti s technickými a organizačními bezpečnostními opatřeními uvedenými v dodatku 2 k této smlouvě;
- d) po vyhodnocení požadavků práva rozhodného pro ochranu údajů jsou bezpečnostní opatření dostatečná k zajištění ochrany osobních údajů před náhodným či protiprávním zničením nebo před náhodnou ztrátou, úpravou, neoprávněným zveřejněním či přístupem, zejména v případech, kdy v souvislosti se zpracováním dochází k předávání údajů po síti, nebo před všemi ostatními protiprávními způsoby zpracování, a že tato opatření zajišťují úroveň bezpečnosti odpovídající rizikům, která v souvislosti se zpracováním hrozí, a povaze údajů, jež mají být chráněny, s ohledem na stav techniky a nákladnost jejich zavedení;
- e) zajistí dodržování bezpečnostních opatření;
- f) budou-li součástí předávání i zvláštní kategorie údajů, subjekt údajů byl nebo bude informován před předáním nebo co nejdříve poté, že jeho údaje mohou být předávány do třetí země, která neposkytuje odpovídající ochranu ve smyslu směrnice 95/46[...];
- g) předá oznámení obdržené od dovozce údajů nebo případného dílčího zpracovatele podle doložky 5 písm. b) a doložky 8 odst. 3 orgánu dozoru pro ochranu údajů, pokud se vývozce údajů rozhodne pokračovat v předávání nebo odvolat jeho pozastavení;
- h) na požádání poskytne subjektům údajů kopii doložek, s výjimkou dodatku 2 a souhrnného popisu bezpečnostních opatření, a rovněž kopii případné smlouvy o službách dílčího zpracování, kterou je nutno uzavřít v souladu s doložkami, pokud doložky nebo smlouva neobsahují obchodní informace, v tomto případě je možno tyto obchodní informace vynechat;
- i) v případě dílčího zpracování je činnost spojená se zpracováním údajů vykonávána v souladu s doložkou 11 dílčím zpracovatelem, který zajišťuje přinejmenším stejnou úroveň ochrany osobních údajů a práv subjektu údajů jako dovozce údajů podle doložek, a
- j) zajistí shodu s doložkou 4 písm. a) až i).“

28. Doložka 5 stanovená v téže příloze, nadepsaná „Povinnosti dovozce údajů⁽¹⁾“, uvádí:

„Dovozce údajů se zavazuje a zaručuje, že:

- a) osobní údaje bude zpracovávat pouze jménem vývozce údajů a v souladu s jeho pokyny a s těmito doložkami; nebude-li moci dodržování pokynů a doložek z jakýchkoli důvodů zajistit, zavazuje se o tom neprodleně informovat vývozce údajů, který je v takovém případě oprávněn pozastavit předávání údajů a/nebo odstoupit od smlouvy;
- b) nemá důvod se domnívat, že mu právní předpisy, kterým podléhá, brání plnit pokyny vývozce údajů a jeho povinnosti vyplývající ze smlouvy a že v případě změny těchto právních předpisů, která by mohla mít výrazně nepříznivý dopad na ochranná opatření [záruky] a závazky stanovené doložkami, oznámí neprodleně tuto změnu vývozci údajů, který je v takovém případě oprávněn pozastavit předávání údajů a/nebo odstoupit od smlouvy;
- c) před zpracováním předaných osobních údajů učinil organizační a technická bezpečnostní opatření uvedená v dodatku 2;

d) oznámí vývozci údajů neprodleně:

- i) veškeré právně závazné požadavky na zveřejnění osobních údajů ze strany donucovacího orgánu, není-li to jinak zakázáno, například trestním právem, aby byla zajištěna důvěrnost vyšetřování v rámci výkonu práva;
 - ii) veškeré případy získání náhodného nebo neoprávněného přístupu a
 - iii) veškeré žádosti obdržené přímo od subjektů údajů, aniž by na tyto žádosti reagoval, ledaže k tomu byl jinak oprávněn;
- e) vyřídí neprodleně a řádně veškeré dotazy vývozce údajů týkající se jím prováděného zpracování osobních údajů, které jsou předmětem přenosu, a že se bude řídit v souvislosti se zpracováním předávaných údajů názorem orgánu dozoru;
- f) na žádost vývozce údajů umožní přezkoumání činností spojených se zpracováním údajů podle doložek ve svých zařízeních na zpracování údajů, které provede vývozce údajů nebo kontrolní orgán složený z nezávislých členů s požadovanou odbornou kvalifikací, kteří budou vázáni povinností zachovat mlčenlivost a vybráni vývozcem údajů, popřípadě po dohodě s orgánem dozoru;

[...]"

29. Podle poznámky pod čarou 1, na kterou odkazuje nadpis doložky 5 obsažené v příloze rozhodnutí 2010/87, platí:

„Povinné požadavky vnitrostátních právních předpisů vztahujících se na dovozce údajů, které nepřekračují rámec toho, co je nezbytné v demokratické společnosti, na základě jednoho ze zájmů uvedených v čl. 13 odst. 1 směrnice 95/46[...], tzn. představují-li opatření nezbytná k zajištění bezpečnosti státu, obrany, veřejné bezpečnosti, předcházení trestným činům a jejich vyšetřování, odhalování a stíhání nebo nedodržování deontologických pravidel pro regulovaná povolání, významného hospodářského nebo finančního zájmu státu nebo ochrany subjektu údajů nebo práv a svobod druhých, nejsou v rozporu se standardními smluvními doložkami. Příkladem takových povinných požadavků, které nepřekračují rámec toho, co je nezbytné v demokratické společnosti, jsou mimo jiné mezinárodně uznané sankce, požadavky na vykazování daní či požadavky na předkládání zpráv o boji proti legalizaci výnosů z trestné činnosti.“

30. Doložka 6 obsažená v této příloze, nadepsaná „Odpovědnost“, zní následovně:

„1. Strany se dohodly, že subjekt údajů, který utrpěl v důsledku porušení povinností uvedených v doložce 3 nebo doložce 11 škodu způsobenou kteroukoli ze stran nebo dílčím zpracovatelem, je oprávněn obdržet od vývozce údajů za utrpěnou škodu náhradu.

2. Nemůže-li subjekt údajů uplatňovat v souladu s odstavcem 1 nárok na odškodnění vůči vývozci údajů pro porušení některé z povinností dovozce údajů nebo jeho dílčího zpracovatele uvedených v doložce 3 a 11, protože vývozce údajů fakticky zmizel, z právního hlediska zanikl nebo je v platební neschopnosti, dovozce údajů se zavazuje, že subjekt údajů smí uplatňovat nároky vůči dovozci údajů, jako by byl vývozcem údajů, ledaže případný nástupnický subjekt převzal na základě smlouvy nebo právních předpisů veškeré právní povinnosti vývozce údajů, přičemž v tomto případě může subjekt uplatňovat svá práva vůči tomuto subjektu.

[...]"

31. Doložka 7 uvedená ve zmíněné příloze, nadepsaná „Mediace a soudní příslušnost“, stanoví:

„1. Dovozece údajů se zavazuje, že uplatní-li proti němu subjekt údajů práva ve prospěch třetí strany a/nebo uplatní-li nárok na náhradu škody podle těchto doložek, přistoupí dovozce údajů na rozhodnutí subjektu údajů:

- a) předat spor k mediaci prováděné nezávislou osobou nebo popřípadě orgánem dozoru;
- b) předat spor soudům v členském státě, ve kterém je vývozce údajů usazen.

2. Strany se dohodly, že rozhodnutím subjektu údajů nebudou dotčena jeho hmotná ani procesní práva při podávání soudních žalob v souladu s ostatními ustanoveními vnitrostátního nebo mezinárodního práva.“

32. Doložka 9 obsažená v téže příloze, nadepsaná „Rozhodné právo“, stanoví, že se smluvní doložky řídí právem členského státu, ve kterém je usazen vývozce údajů.

D. Rozhodnutí o štítu na ochranu soukromí

33. Článek 25 odst. 6 směrnice 95/46 sloužil jako základ pro dvě po sobě jdoucí rozhodnutí Komise, v nichž Komise konstatovala, že Spojené státy zajišťují odpovídající úroveň ochrany osobních údajů předávaných podnikům usazeným ve Spojených státech, které prostřednictvím vlastního osvědčení prohlásily, že přistoupí k zásadám uvedeným v těchto rozhodnutích.

34. Nejprve Komise přijala rozhodnutí 2000/520/ES o odpovídající ochraně poskytované podle zásad „bezpečného přístavu“ a s tím souvisejících „často kladených otázek“ vydaných Ministerstvem obchodu Spojených států¹¹. V rozsudku ze dne 6. října 2015, Schrems¹², Soudní dvůr rozhodl o neplatnosti tohoto rozhodnutí.

35. V návaznosti na tento rozsudek přijala Komise následně rozhodnutí o štítu na ochranu soukromí.

36. Článek 1 tohoto rozhodnutí stanoví:

„1. Pro účely čl. 25 odst. 2 směrnice 95/46[...] Spojené státy zajišťují odpovídající úroveň ochrany osobních údajů předávaných z Unie organizacím ve Spojených státech v rámci štítu EU-USA na ochranu soukromí.

2. Štít EU-USA na ochranu soukromí sestává ze zásad vydaných Ministerstvem obchodu dne 7. července 2016, které jsou obsaženy v příloze II, a oficiálních prohlášení a závazků, které jsou obsaženy v přílohách I a III až VII.

3. Pro účely odstavce 1 jsou osobní údaje předávány v rámci štítu EU-USA na ochranu soukromí, jsou-li předávány z Unie organizacím ve Spojených státech uvedeným na „seznamu organizací štítu na ochranu soukromí“, který vede a zpřístupňuje Ministerstvo obchodu USA v souladu s částí I a III zásad uvedených v příloze II.“

11 – Rozhodnutí ze dne 26. července 2000 podle směrnice [95/46] (Úř. věst. 2000, L 215, s. 7; Zvl. vyd. 16/001, s. 119, dále jen „rozhodnutí o ‚bezpečném přístavu‘“).

12 – C-362/14 (EU:C:2015:650, dále jen „rozsudek Schrems“).

37. Příloha III A tohoto rozhodnutí, nadepsaná „Mechanismus ombudsmana ve věcech štítu na ochranu soukromí v souvislosti se signálovým zpravodajstvím“, přiložená k dopisu Johna Kerryho, tehdejšího Secretary of State (ministr zahraničních věcí, Spojené státy), ze dne 7. července 2016, obsahuje memorandum, které stanoví nový proces mediace u „vedoucího koordinátora pro mezinárodní informační diplomacii“ (dále jen „ombudsman“), jmenovaného ministrem zahraničních věcí.

38. Podle tohoto memoranda byl tento proces zaveden s cílem „usnadn[it] zpracovávání žádostí, které se týkají přístupu k údajům pro účely národní bezpečnosti v případě údajů předaných z [Unie] do Spojených států v rámci štítu na ochranu soukromí, standardních smluvních doložek, závazných podnikových pravidel, ‚odchylek‘ nebo ‚možných budoucích odchylek‘ zavedenými postupy podle platných zákonů a politiky Spojených států a odpovědí na uvedené žádosti“.

III. Spor v původním řízení, předběžné otázky a řízení před Soudním dvorem

39. M. Schrems, rakouský státní příslušník s bydlištěm v Rakousku, je uživatelem sociální sítě Facebook. Všichni uživatelé této sociální sítě s bydlištěm na území Unie musí při registraci uzavřít smlouvu se společností Facebook Ireland, jež je dceřinou společností společnosti Facebook Inc., která je usazena ve Spojených státech. Osobní údaje těchto uživatelů jsou zcela nebo zčásti předávány serverům náležejícím společnosti Facebook Inc., které se nacházejí na území Spojených států, kde jsou tyto údaje předmětem zpracování.

40. Dne 25. června 2013 podal M. Schrems u DPC stížnost, kterou se v podstatě domáhal, aby bylo společnosti Facebook Ireland zakázáno předávat osobní údaje, které se ho týkají, do Spojených států. Ve stížnosti tvrdil, že právní předpisy a postupy v této třetí zemi nezajišťují dostatečnou ochranu osobních údajů uchovávaných na jejím území před sledováním prováděným v této zemi orgány veřejné moci. M. Schrems se v tomto ohledu odvolával na zjištění učiněná Edwardem Snowdenem o činnosti zpravodajských služeb Spojených států, konkrétně činnosti National Security Agency (NSA) (Národní bezpečnostní agentura, Spojené státy).

41. Tato stížnost byla zamítnuta zejména z důvodu, že jakákoli otázka týkající se odpovídající ochrany zajištěné ve Spojených státech musí být rozhodnuta v souladu s rozhodnutím o „bezpečném přístavu“. V tomto rozhodnutí Komise konstatovala, že tato třetí země poskytuje odpovídající úroveň ochrany osobních údajů předávaných podnikům nacházejícím se na jejím území, které přistoupily k zásadám stanoveným v uvedeném rozhodnutí.

42. M. Schrems podal žalobu proti rozhodnutí o zamítnutí své stížnosti k High Court (Vrchní soud). Uvedený soud rozhodl, že i když M. Schrems formálně nezpochybnil platnost rozhodnutí o „bezpečném přístavu“, jeho stížnost ve skutečnosti napadala legalitu režimu zavedeného tímto rozhodnutím. Za těchto podmínek uvedený soud položil Soudnímu dvoru otázky, které se v podstatě týkaly toho, zda jsou orgány členských států pověřené ochranou údajů (dále jen „orgány dozoru“) při vyřizování stížnosti týkající se ochrany práv a svobod osob v souvislosti se zpracováním osobních údajů, které se jich týkají a které byly předány do třetího státu, vázány zjištěními týkajícími se odpovídající úrovně ochrany poskytované tímto třetím státem provedenými Komisí podle čl. 25 odst. 6 směrnice 95/46, i když stěžovatel tato zjištění zpochybňuje.

43. Poté, co Soudní dvůr v bodech 51 a 52 rozsudku Schrems rozhodl, že rozhodnutí o odpovídající ochraně zavazuje orgány dozoru po dobu, dokud není toto rozhodnutí prohlášeno za neplatné, uvedl v bodech 63 a 65 tohoto rozsudku toto:

„63. [...] [U]vedený [musí] orgán posoudit tuto žádost s veškerou náležitou péčí v případě, že se osoba, jejíž osobní údaje byly nebo by mohly být předány do třetí země, na kterou se vztahuje rozhodnutí Komise na základě čl. 25 odst. 6 směrnice 95/46, obrátí na vnitrostátní orgán dozoru se žádostí týkající se ochrany svých práv a svobod v souvislosti se zpracováním těchto údajů a v rámci této žádosti zpochybní[...] slučitelnost tohoto rozhodnutí s ochranou soukromí a základních práv a svobod osob.

[...]

65. Má-li uvedený orgán [...] za to, že výtky uplatněné [touto osobou] jsou opodstatněné, musí mít tento orgán v souladu s čl. 28 odst. 3 prvním pododstavcem třetí odrážkou směrnice 95/46, ve spojení zejména s čl. 8 odst. 3 Listiny, možnost obrátit se na soud. V tomto ohledu přísluší vnitrostátnímu normotvůrci, aby stanovil procesní prostředky, které by dotyčnému vnitrostátnímu orgánu dozoru umožnily uplatnit výtky, jež považuje za opodstatněné, před vnitrostátními soudy, aby tyto soudy v případě, že sdílejí pochybnosti vyjádřené tímto orgánem o platnosti rozhodnutí Komise, předložily žádost o rozhodnutí o předběžné otázce za účelem přezkumu platnosti tohoto rozhodnutí.“

44. V uvedeném rozsudku Soudní dvůr rovněž přezkoumal platnost rozhodnutí o „bezpečném přístavu“ s ohledem na požadavky, které vyplývají ze směrnice 95/46, vykládané ve světle Listiny. Na závěr tohoto přezkumu toto rozhodnutí prohlásil za neplatné¹³.

45. V návaznosti na rozsudek Schrems zrušil předkládající soud rozhodnutí, kterým DPC zamítl stížnost M. Schremse, a vrátil ji DPC k novému projednání a rozhodnutí. DPC zahájil šetření a vyzval M. Schremse, aby přeformuloval svou stížnost vzhledem ke zrušení platnosti rozhodnutí o „bezpečném přístavu“.

46. Za tímto účelem M. Schrems požádal společnost Facebook Ireland, aby určila právní základy, na kterých je založeno předávání osobních údajů uživatelů sociální sítě Facebook z Unie do Spojených států. Společnost Facebook Ireland, aniž určila všechny právní základy, o které se opírá, odkázala na dohodu o předávání a zpracování údajů (*data transfer processing agreement*) uzavřenou mezi ní a společností Facebook Inc., použitelnou od 20. listopadu 2015, a dovolávala se rozhodnutí 2010/87.

47. M. Schrems ve své přeformulované stížnosti tvrdí, že doložky obsažené v této dohodě nejsou v souladu se standardními smluvními doložkami, které jsou obsaženy v příloze rozhodnutí 2010/87. M. Schrems kromě toho tvrdí, že tyto smluvní doložky nemohou v žádném případě zakládat předání osobních údajů, které se ho týkají, do Spojených států. Je tomu tak proto, že americké právo ukládá společnosti Facebook Inc. povinnost poskytovat osobní údaje uživatelů k dispozici americkým orgánům, jako jsou NSA a Federal Bureau of Investigation (FBI) (Federální úřad pro vyšetřování, Spojené státy), v rámci sledovacích programů, které narušují výkon práv zaručených v člancích 7, 8 a 47 Listiny. M. Schrems tvrdí, že žádný procesní prostředek neumožňuje subjektům údajů uplatnit svá práva na respektování soukromého života a ochranu osobních údajů. Za těchto podmínek M. Schrems navrhl DPC, aby pozastavil toto předávání na základě článku 4 rozhodnutí 2010/87.

48. Společnost Facebook Ireland v rámci šetření DPC uznala, že nadále předává osobní údaje uživatelů sociální sítě Facebook pobývajících v Unii do Spojených států a že se za tímto účelem z velké části opírá o standardní smluvní doložky uvedené v příloze rozhodnutí 2010/87.

¹³ – Viz rozsudek Schrems (bod 106).

49. Cílem šetření DPC bylo určit jednak to, zda Spojené státy zajišťují odpovídající ochranu osobních údajů občanů Unie, a jednak, v případě záporné odpovědi, to, zda rozhodnutí SSD představují vhodné záruky, co se týče ochrany základních práv a svobod těchto občanů.

50. V tomto ohledu DPC v návrhu rozhodnutí (*draft decision*) dospěl k předběžnému závěru, že americké právo neposkytuje účinné procesní prostředky ve smyslu článku 47 Listiny občanům Unie, jejichž údaje jsou předávány do Spojených států, kde existuje nebezpečí, že mohou být zpracovány americkými agenturami pro účely národní bezpečnosti způsobem neslučitelným s články 7 a 8 Listiny. Záruky stanovené v doložkách uvedených v příloze rozhodnutí SSD tuto mezeru nenapravují, jelikož nejsou pro orgány či agentury Spojených států závazné a přiznávají subjektům údajů pouze smluvní práva proti vývozcí nebo dovozci údajů.

51. Za těchto podmínek se DPC domníval, že nemůže rozhodnout o stížnosti M. Schremse, aniž Soudní dvůr přezkoumá platnost rozhodnutí SSD. DPC proto v souladu s tím, co stanoví bod 65 rozsudku Schrems, zahájil řízení u předkládajícího soudu směřující k tomu, aby tento soud, pokud bude sdílet pochybnosti DPC, předložil Soudnímu dvoru žádost o rozhodnutí o předběžné otázce týkající se platnosti těchto rozhodnutí.

52. Vládě Spojených států, Electronic Privacy Information Centre (VIPO), Business Software Alliance (BSA) a Digitaleurope bylo povoleno vstoupit do řízení před předkládajícím soudem jako vedlejší účastníci.

53. Za účelem určení, zda sdílí pochybnosti vyjádřené DPC o platnosti rozhodnutí SSD, obdržel High Court (Vrchní soud) důkazy předložené stranami sporu a vyslechl argumenty předložené těmito stranami, jakož i vedlejšími účastníky. Předmětem důkazů předložených znalci byla zejména ustanovení práva Spojených států. V irském právu je zahraniční právo považováno za skutkovou otázku, která musí být prokázána stejným způsobem jako jakákoli jiná skutečnost. Na základě těchto důkazů předkládající soud posoudil ustanovení práva Spojených států, která povolují sledování vládními orgány a agenturami, fungování dvou veřejně uznávaných sledovacích programů („PRISM“ a „Upstream“), různé procesní prostředky poskytnuté jednotlivcům, jejichž práva byla porušena prostřednictvím sledování, jakož i systémové záruky a kontrolní mechanismy. Uvedený soud zaznamenal výsledky tohoto posouzení v rozsudku ze dne 3. října 2017, připojeném k jeho předkládacímu usnesení [dále jen „rozsudek High Court (Vrchní soud) ze dne 3. října 2017“].

54. V tomto rozsudku předkládající soud mezi právními základy povolujícími odposlechy zahraničních komunikací americkými zpravodajskými službami odkazuje na článek 702 Foreign Intelligence Surveillance Act (FISA) (zákon o dohledu nad zahraničními zpravodajskými službami) a Executive Order 12333 (nařízení prezidenta č. 12333, dále jen „EO 12333“).

55. Podle zjištění provedených v uvedeném rozsudku článek 702 FISA umožňuje Attorney General (státní zástupce, Spojené státy) a Director of National Intelligence (DNI) (ředitel národního zpravodajství, Spojené státy), aby za účelem získání informací v oblasti zahraničního zpravodajství společně na dobu jednoho roku povolili sledování osob, které nejsou americkými občany a nemají trvalé bydliště ve Spojených státech (tzv. „neamerické osoby“), pokud je důvodné se domnívat, že se nacházejí mimo území Spojených států¹⁴. Podle FISA pojem „zahraniční zpravodajství“ označuje informace o schopnosti vlády chránit se před cizími útoky, terorismu, šíření zbraní hromadného ničení, jakož i vedení zahraničních věcí Spojených států¹⁵.

14 – 50 U. S. C. 1881 (a).

15 – 50 U. S. C. 1881 (e).

56. Tato roční povolení, jakož i postupy, které upravují zacílení osob, které mají být sledovány, a zpracování („minimalizaci“) shromážděných informací¹⁶, musí být schváleny Foreign Intelligence Surveillance Court (FISC) (Soud pro uplatňování zákona FISA, Spojené státy). Zatímco „tradiční“ sledování prováděné na základě jiných ustanovení FISA vyžaduje, aby byla prokázána „pravděpodobná příčina“ vyvolávající podezření, že sledované osoby náležejí k zahraniční moci nebo jsou jejími agenty, sledování prováděné na základě článku 702 FISA nepodléhá prokázání takové „pravděpodobné příčiny“, ani schválení zacílení určených osob Soudem pro uplatňování zákona FISA. Mimoto rovněž podle zjištění předkládajícího soudu se postupy pro minimalizaci neuplatní ve vztahu k neamerickým osobám nacházejícím se mimo Spojené státy.

57. V praxi poté, co bylo povolení Soudem pro uplatňování zákona FISA uděleno, zašle NSA poskytovatelům služeb elektronických komunikací, usazeným ve Spojených státech, směrnice obsahující kritéria pro vyhledávání, nazvaná „selektory“, spojená s cílovými osobami (jako například telefonní čísla nebo emailové adresy). Tito poskytovatelé jsou poté povinni předat údaje, které odpovídají selektorům NSA, a musí zachovávat mlčenlivost ve vztahu ke směrnicím, které jsou jim určeny. Mohou podat u Soudu pro uplatňování zákona FISA návrh na změnu nebo odmítnutí směrnice NSA. Rozhodnutí Soudu pro uplatňování zákona FISA může být napadeno odvoláním u Foreign Intelligence Surveillance Court of Review (FISCR) (Odvolací soud pro uplatňování zákona FISA, Spojené státy).

58. High Court (Vrchní soud) konstatoval, že článek 702 FISA slouží jako právní základ pro programy PRISM a Upstream.

59. V rámci programu PRISM mají poskytovatelé služeb elektronických komunikací povinnost předložit NSA veškerou komunikaci „pocházející od“ selektoru, který NSA sdělila, nebo „určenou pro“ takový selektor. Část této komunikace je předána FBI a Central Intelligence Agency (CIA) (Ústřední zpravodajská služba, Spojené státy). V roce 2015 bylo sledováno 94 386 osob a v roce 2011 získala vláda Spojených států 250 milionů komunikací v rámci tohoto programu.

60. Program Upstream spočívá v povinné pomoci podniků provozujících „páteří sítě“ – a sice kabelovou síť, přepínače a směrovače – na kterých probíhají telefonní hovory a internetová komunikace. Tyto podniky jsou povinny umožnit NSA kopírování a filtrování internetových toků za účelem získání komunikace „pocházející od“, „určené pro“ nebo „týkající se“ selektoru uvedeného ve směrnici této agentury. Komunikace „týkající se“ selektoru označují tu komunikaci, která odkazuje na tento selektor, aniž se jí uvedená neamerická osoba, která je spojena s uvedeným selektorem, nutně účastní. I když ze stanoviska Soudu pro uplatňování zákona FISA ze dne 26. dubna 2017 vyplývá, že od tohoto data americká vláda již neshromažďuje a nezískává komunikace „týkající se“ určitého selektoru, není v tomto stanovisku uvedeno, že by NSA zastavila kopírování a filtrování komunikačních toků, které jsou přenášeny prostřednictvím jejího mechanismu sledování. Program Upstream předpokládá přístup NSA k metadatům i k obsahu komunikací. Od roku 2011 NSA v rámci programu Upstream shromáždila přibližně 26,5 milionu komunikací ročně, což však představuje jen malou část komunikací, které podléhají procesu filtrování provedeného na základě tohoto programu.

16 – Předkládající soud konstatoval, že postupy pro zacílení se týkají způsobu, jakým výkonná moc určuje, zda je důvodné se domnívat, že jednotlivec je neamerickou osobou, která se nachází mimo Spojené státy, a že zacílení tohoto jednotlivce může vést k získání informací v oblasti zahraničního zpravodajství. Postupy pro minimalizaci zahrnují získávání, zajištění, používání a šíření jakékoli neveřejné informace týkající se americké osoby získané na základě článku 702 FISA.

61. Kromě toho podle zjištění High Court (Vrchní soud) EO 12333 povoluje sledování elektronických komunikací mimo území Spojených států tím, že umožňuje přístup za účelem zahraničního zpravodajství k údajům, které „směřují“ na toto území nebo tímto územím „procházejí“, aniž by na něm byla určena ke zpracování, jakož i shromažďování a uchovávání těchto údajů. EO 12333 definuje pojem „zahraniční zpravodajství“ jako zahrnující informace o kapacitách, záměrech nebo činnostech zahraničních vlád, zahraničních organizací nebo zahraničních osob¹⁷.

62. EO 12333 zmocňuje NSA k přístupu k podmořským kabelům, které se nacházejí na dně Atlantického oceánu a prostřednictvím kterých jsou údaje předávány z Unie do Spojených států, tedy před tím, než tyto údaje přijdou do Spojených států a podléhaly by z tohoto důvodu ustanovením FISA. Neexistuje však žádný důkaz o jakémkoli programu prováděném na základě tohoto nařízení prezidenta.

63. Ačkoli EO 12333 stanoví omezení týkající se shromažďování, zajišťování a šíření informací, nevztahují se tyto meze na neamerické osoby. Na tyto osoby se vztahují pouze záruky uvedené v Presidential Policy Directive 28 (strategická prezidentská směrnice č. 28, dále jen „PPD 28“), která se vztahuje na všechny činnosti shromažďování a používání informací v oblasti zahraničního zpravodajství elektromagnetického původu. PPD 28 stanoví, že respektování soukromého života je nedílnou součástí úvah, které je třeba vzít v úvahu při plánování těchto činností, že jediným účelem shromažďování musí být získání informací v oblasti zahraničního zpravodajství, jakož i kontrarozvědky a že uvedené činnosti musí být „v nejvyšší možné míře uzpůsobeny na míru“.

64. Podle předkládajícího soudu nejsou činnosti NSA založené na EO 12333, které může být kdykoliv změněno nebo zrušeno prezidentem Spojených států, upraveny zákonem, nejsou předmětem soudního dohledu a nelze je napadnout procesními prostředky u soudů.

65. Na základě těchto zjištění má tento soud za to, že Spojené státy provádějí rozsáhlé a bez rozdílu uplatňované zpracování osobních údajů, které může subjekty údajů vystavovat riziku porušení práv, která pro ně vyplývají z článků 7 a 8 Listiny.

66. Kromě toho uvedený soud uvádí, že občané Unie nemají přístup k týmž soudním žalobám proti nedovolenému zpracování svých osobních údajů ze strany amerických orgánů, jako mají američtí státní příslušníci. Čtvrtý dodatek k Ústavě Spojených států, který představuje nejvýznamnější ochranu před protiprávním sledováním, je nepoužitelný na občany Unie, kteří nevykazují významné dobrovolné spojení se Spojenými státy. Nicméně i když mají tyto občany k dispozici některé jiné žaloby, naráží na významné překážky.

67. Konkrétně článek III Ústavy Spojených států stanoví jako podmínku pro podání žaloby k federálnímu soudu prokázání právního zájmu dotčené osoby na podání žaloby (*standing*). Právní zájem na podání žaloby zejména předpokládá, že tato osoba prokáže, že jí vznikla skutečná škoda, která je jednak konkrétní a rozlišitelná a jednak skutečná a bezprostřední. S odkazem mimo jiné na rozsudek Supreme Court of the United States (Nejvyšší soud Spojených států), *Clapper v. Amnesty International US*¹⁸, má předkládající soud za to, že tato podmínka je v praxi příliš obtížně splnitelná, zejména s ohledem na neexistenci jakékoli povinnosti informovat subjekty údajů o opatřeních

17 – EO 12333, bod 3.5 písm. e).

18 – 133 S.Ct. 1138 (2013).

přijatých ve vztahu k nim¹⁹. Část žalob, které mají k dispozici občané Unie, podléhá navíc jiným omezujícím podmínkám, jako je nutnost prokázat finanční újmu. Svrchovaná imunita přiznaná zpravodajským agenturám a klasifikace dotyčných informací rovněž brání výkonu některých procesních prostředků²⁰.

68. High Court (Vrchní soud) navíc poukazuje na různé mechanismy kontroly a dozoru nad činnostmi zpravodajských agentur.

69. Patří mezi ně mechanismus roční certifikace programů založených na článku 702 FISA prostřednictvím Soudu pro uplatňování zákona FISA, v jehož rámci však uvedený soud neschvaluje jednotlivé selektory. Kromě toho žádný předchozí soudní přezkum neupravuje shromažďování informací týkajících se zahraničního zpravodajství na základě EO 12333.

70. Předkládající soud kromě toho odkazuje na několik mechanismů mimosoudního dohledu nad zpravodajskými činnostmi. Uvádí zejména úlohu Inspectors General (generální inspektoři, Spojené státy), kteří jsou v rámci každé zpravodajské agentury pověřeni dohledem nad činnostmi sledování. Kromě toho Privacy and Civil Liberties Oversight Board (PCLOB) (Rada pro dohled nad soukromím a občanskými svobodami, Spojené státy), nezávislá agentura v rámci výkonné moci, přijímá zprávy od osob určených v rámci každé agentury za zmocněnce občanskoprávních svobod nebo soukromí (*civil liberties or privacy officers*). PCLOB připravuje pravidelně zprávy pro parlamentní inspektory a prezidenta. Dotčené agentury musí oznamovat události týkající se porušení pravidel a postupů upravujících shromažďování zahraničního zpravodajství zejména DNI. Tyto události jsou rovněž oznamovány Soudu pro uplatňování zákona FISA. Kongres Spojených států rovněž prostřednictvím výborů pro zpravodajství Kongresu a Senátu nese odpovědnost za kontrolu zahraničního zpravodajství.

71. High Court (Vrchní soud) nicméně zdůrazňuje zásadní rozdíl zaprvé mezi pravidly, která mají zajistit, aby údaje byly získávány v souladu s právními předpisy a aby jakmile jsou získány, nebyly zneužity, a zadruhé dostupnými procesními prostředky, pokud jsou tato pravidla porušena. Ochrana základních práv subjektů údajů je zajištěna pouze tehdy, když jim účinné procesní prostředky umožňují uplatnit jejich práva v případě porušení uvedených pravidel.

72. Za těchto podmínek považuje předkládající soud za opodstatněné argumenty, kterých se dovolává DPC a podle nichž omezení, která ukládá americké právo z hlediska práva osob, jejichž údaje jsou předávány z Unie, podat žalobu, nerespektují podstatu práva zaručeného článkem 47 Listiny a v každém případě představují nepřiměřené zásahy do výkonu tohoto práva.

73. Podle High Court (Vrchní soud) skutečnost, že vláda Spojených států zavedla mechanismus ombudsmana popsany v rozhodnutí o štítu na ochranu soukromí, toto posouzení nezpochybnuje. Tento soud poté, co zdůraznil, že tento mechanismus je dostupný občanům Unie, kteří mají za to, že jejich údaje byly předány v souladu s rozhodnutími SSD²¹, poznamenal, že ombudsman není soudem, který splňuje požadavky článku 47 Listiny, a zejména není nezávislý na výkonné moci²². Uvedený soud má rovněž pochybnosti o tom, že zásah ombudsmana, jehož rozhodnutí nelze napadnout žalobou, představuje účinný právní prostředek. Tento zásah totiž neumožňuje osobám, jejichž osobní údaje byly protiprávně shromažďovány, zpracovávány nebo sdíleny, aby se domáhaly náhrady škody nebo příkazu ukončit protiprávní jednání, jelikož ombudsman nepotvrzuje ani nepopírá, že vůči žalobci bylo vydáno opatření elektronického sledování.

19 – Předkládající soud však konstatoval, že u zásady, podle které není požadováno oznámení osobě, která je sledována, se uplatní výjimka, pokud americká vláda hodlá použít údaje shromážděné na základě článku 702 FISA proti této osobě v rámci trestního nebo správního řízení.

20 – Předkládající soud zejména uvedl, že i když Judicial Redress Act (JRA) (zákon o soudní ochraně) rozšířil na občany Unie ustanovení Privacy Act (zákon o ochraně soukromí), který umožňuje fyzickým osobám přístup k informacím, které se jich týkají a které mají v držení některé agentury v souvislosti s některými třetími zeměmi, NSA nespadá mezi agentury určené na základě JRA.

21 – Předkládající soud v tomto ohledu odkazuje na přílohu III A rozhodnutí o štítu na ochranu soukromí (viz body 37 a 38 tohoto stanoviska).

22 – Předkládající soud se dovolává rozsudku ze dne 27. ledna 2005, Denuit a Cordenier (C-125/04, EU:C:2005:69, bod 12).

74. Po uvedení svých obav o podstatné rovnocennosti mezi zárukami stanovenými americkým právem a požadavky vyplývajícími z článků 7, 8 a 47 Listiny vyslovil předkládající soud pochybnosti o tom, zda smluvní doložky stanovené v rozhodnutích SSD – které ze své povahy nejsou závazné pro americké orgány – mohou nicméně zajistit ochranu základních práv subjektů údajů. Tento soud z toho vyvodil, že sdílí pochybnosti DPC týkající se platnosti těchto rozhodnutí.

75. V tomto ohledu má předkládající soud zejména za to, že čl. 28 odst. 3 směrnice 95/46, na který odkazuje článek 4 rozhodnutí 2010/87, v rozsahu, v němž přiznává orgánům dozoru pravomoc pozastavit nebo zakázat předávání založená na smluvních doložkách stanovených v uvedeném rozhodnutí, nepostačuje k rozptýlení těchto pochybností. Mimo to, že podle jeho názoru má tato pravomoc pouze diskreční povahu, se předkládající soud ve světle bodu 11 odůvodnění rozhodnutí 2010/87 zabývá tím, zda je možné tuto pravomoc vykonat, jestliže se zjištěné nedostatky netýkají zvláštního a výjimečného případu, ale mají obecný a systémový charakter²³. Rovněž se domnívá, že nebezpečí, že v různých členských státech budou vydána rozdílná rozhodnutí, může bránit tomu, aby bylo zjištění takových nedostatků svěřeno kontrolním orgánům.

76. Za těchto podmínek se High Court (Vrchní soud, Irsko) rozhodnutím ze dne 4. května 2018²⁴, došlým kanceláři Soudního dvora dne 9. května 2018, rozhodl přerušit řízení a položit Soudnímu dvoru následující předběžné otázky:

- „1) Za okolností, kdy jsou osobní údaje předávány soukromou společností z členského státu [Unie] soukromé společnosti ve třetí zemi k obchodním účelům podle rozhodnutí [...] 2010/87 a mohou být dále zpracovávány ve třetí zemi orgány této země pro účely národní bezpečnosti, ale také za účelem vymáhání práva a provádění zahraniční politiky třetí země, uplatní se na předávání těchto údajů unijní právo [včetně Listiny základních práv Evropské unie] bez ohledu na ustanovení čl. 4 odst. 2 SEU ohledně národní bezpečnosti a ustanovení čl. 3 odst. 2 první odrážky směrnice 95/46[...] ohledně veřejné bezpečnosti, obrany a bezpečnosti státu?
- 2) a) Je při určování, zda předáním údajů podle rozhodnutí [2010/87] z [Unie] do třetí země, kde mohou být dále zpracovány pro účely národní bezpečnosti, došlo k porušení práv jednotlivce, relevantním srovnávacím kritériem pro účely směrnice:
- i) Listina, SEU, SFEU, směrnice [95/46], [Evropská úmluva o ochraně lidských práv a základních svobod, podepsaná dne 4. listopadu 1950 v Římě (dále jen „EÚLP“)] (nebo jiné ustanovení unijního práva), nebo
- ii) vnitrostátní právní předpisy jednoho nebo více členských států?
- b) Je-li relevantním srovnávacím kritériem písmeno b), mají do něj být zahrnuty i postupy v rámci národní bezpečnosti v jednom nebo více členských státech?

23 – Bod 11 odůvodnění rozhodnutí 2010/87 stanoví: „Orgány dozoru členských států hrají v tomto smluvním mechanismu klíčovou úlohu při zajišťování toho, aby osobní údaje byly po předání náležitě chráněny. Ve výjimečných případech, kdy vývozci údajů odmítnou řádně poučit dovozce údajů nebo kdy jej řádně poučit nemohou a kdy subjektům údajů hrozí bezprostřední riziko závažné újmy, by měly standardní smluvní doložky umožňovat orgánům dovozu prověřit dovozce údajů a dílčí zpracovatele a popřípadě přijmout rozhodnutí, která budou pro dovozce údajů a dílčí zpracovatele závazná. Orgány dozoru by měly mít pravomoc zakázat nebo pozastavit předání nebo předávání údajů uskutečněné na základě standardních smluvních doložek ve výjimečných případech, kdy by předávání uskutečněné na smluvním základě mělo pravděpodobně závažný nepříznivý dopad na ochranná opatření [záruky] a povinnosti vztahující se k zajištění odpovídající ochrany subjektu údajů“.

24 – Společnost Facebook Ireland podala odvolání proti předkládacímu rozhodnutí k Supreme Court (Nejvyšší soud, Irsko). Toto odvolání bylo zamítnuto rozsudkem ze dne 31. května 2019, The Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems, Appeal n° 2018/68 [dále jen „rozsudek Supreme Court (Nejvyšší soud) ze dne 31. května 2019“].

- 3) Měla by být při posuzování, zda třetí země zajišťuje osobním údajům předaným do uvedené země úroveň ochrany vyžadovanou unijním právem pro účely článku 26 směrnice [95/46], úroveň ochrany ve třetí zemi posuzována s odvoláním na:
- a) použitelné předpisy ve třetí zemi vyplývající z jejího vnitrostátního práva nebo mezinárodních závazků a postupy, které mají zajišťovat dodržování uvedených předpisů, včetně profesních pravidel a bezpečnostních opatření dodržovaných ve třetí zemi,
- nebo
- b) právní předpisy uvedené v písmenu a) spolu s těmi správními a regulačními postupy a postupy v oblasti dodržování právních předpisů a ochrannými opatřeními, postupy, protokoly, mechanismy dohledu a mimosoudními prostředky nápravy, které existují ve třetí zemi?
- 4) Vzhledem ke skutkovým zjištěním, která učinil High Court (Vrchní soud) ve vztahu k právním předpisům USA, je porušením práv jednotlivců podle článků 7 nebo 8 Listiny, jsou-li osobní údaje předávány z [Unie] do USA podle rozhodnutí [2010/87]?
- 5) Vzhledem ke skutkovým zjištěním, která učinil High Court (Vrchní soud) ve vztahu k právním předpisům USA, jsou-li osobní údaje předány z [Unie] do USA podle rozhodnutí [2010/87]:
- a) zachovává úroveň ochrany poskytovaná USA podstatu práva jednotlivce na prostředky nápravy před soudem při porušení jeho práv na ochranu osobních údajů, zaručeného článkem 47 Listiny?

Je-li odpověď na písmeno a) kladná,

- b) jsou omezení práva jednotlivce na prostředky nápravy před soudem obsažená v právních předpisech USA v souvislosti s národní bezpečností USA přiměřená ve smyslu článku 52 Listiny a nepřekračují rámec toho, co je nezbytné v demokratické společnosti pro účely národní bezpečnosti?
- 6) a) Jaká úroveň ochrany musí být poskytnuta osobním údajům předávaným do třetí země na základě standardních smluvních doložek přijatých v souladu s rozhodnutím Komise podle čl. 26 odst. 4 směrnice [95/46] s přihlédnutím k jejím ustanovením a zejména článkům 25 a 26 vykládaným ve světle Listiny?
- b) Jaké skutečnosti musí být vzaty v úvahu při posuzování, zda úroveň ochrany poskytovaná údajům předávaným do třetí země podle rozhodnutí [2010/87] splňuje požadavky směrnice a Listiny?
- 7) Vylučuje skutečnost, že standardní smluvní doložky platí mezi vývozcem údajů a dovozcem údajů a nejsou závazné pro vnitrostátní orgány třetí země, které mohou po dovozci údajů požadovat, aby jejich zpravodajským službám zpřístupnil k dalšímu zpracování osobní údaje předané podle ustanovení obsažených v rozhodnutí [2010/87], závěr, že doložky poskytují dostatečné záruky, jak předpokládá čl. 26 odst. 2 směrnice [95/46]?
- 8) Pokud dovozce údajů z třetí země podléhá právním předpisům o sledování, které jsou podle názoru orgánu [dozoru] v rozporu [se standardními smluvními doložkami], s články 25 a 26 směrnice [95/46] nebo s Listinou, je [tento orgán] povinen použít své donucovací pravomoci podle čl. 28 odst. 3 směrnice [95/46] a pozastavit toky údajů, nebo je výkon těchto pravomocí s ohledem na bod 11 odůvodnění [rozhodnutí 2010/87] omezen pouze na výjimečné případy, nebo může [orgán dozoru] využít své diskreční pravomoci a toky údajů nepozastavit?

- 9) a) Je pro účely čl. 25 odst. 6 směrnice [95/46], rozhodnutí [...] o štítu na ochranu soukromí[...] obecně závazné pro [orgány dozoru] a soudy členských států v tom smyslu, že USA zajišťují odpovídající úroveň ochrany ve smyslu čl. 25 odst. 2 směrnice [95/46] na základě svého vnitrostátního práva nebo mezinárodních závazků?
- b) Pokud tomu tak není, jaký význam, pokud vůbec nějaký, má rozhodnutí o štítu na ochranu soukromí při posuzování odpovídající úrovně ochranných opatření poskytovaných v souvislosti s údaji předávanými do USA podle rozhodnutí [2010/87]?
- 10) Vzhledem ke zjištění, která učinil High Court (Vrchní soud) ve vztahu k právním předpisům USA, zaručuje úřad ombudsmana ve věcech štítu na ochranu soukromí podle přílohy [III A] rozhodnutí o štítu na ochranu soukromí ve spojení se stávajícím režimem v USA, že USA poskytují prostředky nápravy subjektům údajů, jejichž osobní údaje jsou předávány do USA podle rozhodnutí [2010/87], které jsou slučitelné s článkem 47 Listiny?
- 11) Porušuje rozhodnutí [2010/87] články 7, 8 nebo 47 Listiny?“

77. DPC, Facebook Ireland, M. Schrems, vláda Spojených států, EPIC, BSA, Digitaleurope, Irsko, belgická, česká, německá, nizozemská, rakouská, polská a portugalská vláda a vláda Spojeného království, Evropský parlament, jakož i Komise předložili Soudnímu dvoru písemná vyjádření. DPC, Facebook Ireland, M. Schrems, vláda Spojených států, EPIC, BSA, Digitaleurope, Irsko, německá, francouzská, nizozemská a rakouská vláda a vláda Spojeného království, Parlament, Komise, jakož i evropský sbor pro ochranu údajů (European Data Protection Board, EDPB) byly zastoupeny na jednání k přednesu řečí, které se konalo dne 9. července 2019.

IV. Analýza

A. Úvodní poznámky

78. V návaznosti na zrušení rozhodnutí o „bezpečném přístavu“ Soudním dvorem v rozsudku Schrems pokračovalo předávání osobních údajů do Spojených států na základě jiných právních základů. Společnosti vyvážející údaje mohly zejména využít smlouvy s dovozci údajů, které zahrnovaly standardní doložky vypracované Komisí. Tyto doložky rovněž slouží jako právní základ pro předávání do mnoha jiných třetích zemí, ohledně kterých Komise nepřijala rozhodnutí o odpovídající úrovni ochrany²⁵. Rozhodnutí o štítu na ochranu soukromí nyní umožňuje podnikům, které autocertifikovaly (samy osvědčily) přijetí zásad v něm uvedených, předávat osobní údaje do Spojených států bez dalších formalit.

79. Jak výslovně uvádí předkládací rozhodnutí a jak zdůraznily BSA, Digitaleurope, Irsko, rakouská a francouzská vláda, Parlament, stejně jako Komise, spor v původním řízení, probíhající před High Court (Vrchní soud), má pouze určit, zda je rozhodnutí, kterým Komise zavedla standardní smluvní doložky, dovolávané na podporu předání uvedených ve stížnosti M. Schremse, a sice rozhodnutí 2010/87²⁶, platné.

25 – BSA tvrdí, že 70 % podniků, které jsou členy této aliance a odpověděly na šetření, prohlásilo, že používá za hlavní základ předávání osobních údajů do třetích zemí standardní smluvní doložky. Digitaleurope se rovněž domnívá, že standardní smluvní doložky představují hlavní právní nástroj uplatňovaný na podporu těchto předávání.

26 – Ačkoli předkládající soud uvádí, že se jeho žádost o rozhodnutí o předběžné otázce týká platnosti tří rozhodnutí SSD, které byly přezkoumány v návrhu rozhodnutí DPC a v rozsudku ze dne 3. října 2017, předběžné otázky odkazují výlučně na rozhodnutí 2010/87. Je tomu tak proto, že společnost Facebook Ireland před uvedeným soudem označila toto rozhodnutí za právní základ pro předávání údajů evropských uživatelů sociální sítě Facebook do Spojených států. Moje analýza se tedy bude týkat pouze uvedeného rozhodnutí.

80. Tento spor vychází ze stížnosti, kterou DPC požádal předkládající soud, aby Soudnímu dvoru předložil předběžnou otázku týkající se platnosti rozhodnutí 2010/87. Podle tvrzení předkládajícího soudu se tak spor v původním řízení týká výkonu opravného prostředku, jehož zavedení Soudní dvůr přikázal členským státům v bodě 65 rozsudku Schrems.

81. Pro připomenutí Soudní dvůr rozhodl v bodě 63 uvedeného rozsudku, že orgán dozoru je povinen s veškerou vyžadovanou řádnou péčí projednat stížnost, v níž osoba, jejíž osobní údaje byly nebo by mohly být předány do třetí země, na kterou se vztahuje rozhodnutí o odpovídající úrovni ochrany, zpochybní slučitelnost tohoto rozhodnutí se základními právy zakotvenými Listinou. Podle bodu 65 uvedeného rozsudku, má-li uvedený orgán za to, že výtky uplatněné v této stížnosti jsou opodstatněné, musí mít tento orgán v souladu s čl. 28 odst. 3 prvním pododstavcem třetí odrážkou směrnice 95/46 (kterému odpovídá čl. 58 odst. 5 GDPR) ve spojení zejména s čl. 8 odst. 3 Listiny možnost obrátit se na soud. V tomto ohledu přísluší vnitrostátnímu zákonodárci, aby stanovil procesní prostředky, které by dotýcnému orgánu dozoru umožnily uplatnit výtky před vnitrostátními soudy, aby tyto soudy v případě, že sdílejí pochybnosti vyjádřené tímto orgánem, předložily žádost o rozhodnutí o předběžné otázce za účelem přezkumu platnosti tohoto rozhodnutí.

82. Stejně jako předkládající soud se domnívám, že tyto závěry se uplatní *per analogiam*, pokud má orgán dozoru při projednávání stížnosti podané u tohoto orgánu pochybnosti o platnosti nikoli rozhodnutí o odpovídající úrovni ochrany, nýbrž takového rozhodnutí, jako je rozhodnutí 2010/87, kterým se stanoví standardní smluvní doložky pro předávání osobních údajů do třetích zemí. Na rozdíl od toho, co tvrdí německá vláda, není významné, zda tyto pochybnosti odpovídají výtkám předloženým tomuto orgánu stěžovatelem, nebo zda tento orgán zpochybní platnost dotčeného rozhodnutí na základě vlastního rozhodnutí. Požadavky vyplývající z čl. 58 odst. 5 GDPR a čl. 8 odst. 3 Listiny, na kterých se zakládá odůvodnění Soudního dvora, se totiž uplatní bez ohledu na právní základ předání uvedeného ve stížnosti podané u orgánu dozoru a na důvody, které vedly tento orgán k pochybnostem o platnosti dotčeného rozhodnutí v rámci projednávání této stížnosti.

83. Je však třeba uvést, že když DPC požádal předkládající soud o to, aby se obrátil na Soudní dvůr kvůli platnosti rozhodnutí 2010/87, bylo to z důvodu, že považoval objasnění ze strany Soudního dvora k této otázce za nezbytné k vyřízení stížnosti, kterou jej M. Schrems žádá, aby vykonal pravomoc, kterou mu svěřuje čl. 28 odst. 3 druhá odrážka směrnice 95/46 – a kterou mu nyní přiznává čl. 58 odst. 2 písm. f) GDPR – a sice pozastavit předávání osobních údajů, které se ho týkají, společností Facebook Ireland společnosti Facebook Inc.

84. Zatímco se spor v původním řízení týká pouze platnosti *in abstracto* rozhodnutí 2010/87, podkladové řízení probíhající před DPC se týká jeho výkonu pravomoci přijmout nápravná opatření v *konkrétním případě*. Navrhnu Soudnímu dvoru, aby se zaměřil na přezkum položených otázek v rozsahu nezbytném pro rozhodnutí o platnosti rozhodnutí 2010/87, jelikož takový přezkum bude postačovat k tomu, aby předkládající soud vyřešil spor, který mu byl předložen²⁷.

85. Před posouzením platnosti tohoto rozhodnutí je třeba odmítnout určité námitky vznesené proti přípustnosti žádosti o rozhodnutí o předběžné otázce.

B. K přípustnosti žádosti o rozhodnutí o předběžné otázce

86. Přípustnost žádosti o rozhodnutí o předběžné otázce byla zpochybněna z různých důvodů, které se v zásadě týkají nepoužitelnosti *ratione temporis* směrnice 95/46, uvedené v předběžných otázkách (oddíl 1), skutečnosti, že řízení před DPC nedosáhlo dostatečně pokročilého stadia k tomu, aby byla odůvodněna jejich potřebnost (oddíl 2), a přetrvávající nejistoty týkající se skutkového rámce popsaného předkládajícím soudem (oddíl 3).

²⁷ – Viz body 167 až 186 tohoto stanoviska.

87. Na tyto námitky nepřipustnosti odpovím s ohledem na domněnku relevance otázek položených Soudnímu dvoru na základě článku 267 SFEU. Podle ustálené judikatury je Soudní dvůr oprávněn odmítnout rozhodnout o žádosti o rozhodnutí o předběžné otázce pouze tehdy, je-li zjevné, že požadovaný výklad unijního práva nemá žádný vztah k realitě nebo předmětu sporu v původním řízení, jestliže se jedná o hypotetický problém nebo také jestliže Soudní dvůr nedisponuje skutkovými a právními poznatky nezbytnými pro užitečnou odpověď na otázky, které jsou mu položeny²⁸.

1. K časové působnosti směrnice 95/46

88. Facebook Ireland namítá nepřipustnost předběžných otázek z důvodu, že odkazují na směrnici 95/46, zatímco tato směrnice byla s účinností od 25. května 2018 zrušena a nahrazena GDPR²⁹.

89. Sdílím názor, že platnost rozhodnutí 2010/87 musí být zkoumána ve světle ustanovení GDPR.

90. V souladu s čl. 94 odst. 2 tohoto nařízení „[o]dkazy na zrušenou směrnici se považují za odkazy na toto nařízení“. Podle mého názoru z toho vyplývá, že rozhodnutí 2010/87 v rozsahu, v němž uvádí jako právní základ čl. 26 odst. 4 směrnice 95/46, musí být chápáno tak, že odkazuje na čl. 46 odst. 2 písm. c) GDPR, který v podstatě přejímá jeho obsah³⁰. V důsledku toho musí být prováděcí rozhodnutí přijatá Komisí na základě čl. 26 odst. 4 směrnice 95/46 před vstupem GDPR v platnost vykládána ve světle tohoto nařízení. Jejich platnost musí být případně posouzena rovněž s ohledem na uvedené nařízení.

91. Tento závěr není zpochybněn judikaturou, podle níž musí být legalita unijního aktu posuzována podle skutkových a právních okolností existujících ke dni, kdy byl tento akt přijat. Tato judikatura se totiž týká přezkumu platnosti unijního aktu s ohledem na skutkové okolnosti relevantní při jeho přijímání³¹ nebo na procesní pravidla, která upravují jeho přijetí³². Soudní dvůr naproti tomu opakovaně přezkoumal platnost aktů sekundárního práva z hlediska hmotněprávních norem vyšší právní síly, které vstoupily v platnost po přijetí těchto aktů³³.

92. Skutečnost, že je ve znění předběžných otázek uveden akt, který již není *ratione temporis* použitelný, sice odůvodňuje přeformulování těchto otázek, avšak nemůže vést k jejich nepřipustnosti³⁴. Jak tvrdili DPC a M. Schrems, odkazy na směrnici 95/46 ve znění předběžných otázek lze ostatně vysvětlit s ohledem na procesní harmonogram projednávané věci, neboť tyto otázky byly Soudnímu dvoru předloženy před vstupem GDPR v platnost.

93. V každém případě ustanovení GDPR, která budou zkoumána pro účely analýzy předběžných otázek – a sice zejména jeho články 45, 46 a 58 – v podstatě až na jemné rozdíly přejímají a rozvíjejí obsah článků 25, 26 a 28 směrnice 95/46. Co se týče jejich relevantních aspektů pro účely rozhodnutí o platnosti rozhodnutí 2010/87, nevidím žádný důvod přiznat těmto ustanovením GDPR jiný dosah, než mají odpovídající ustanovení směrnice 95/46³⁵.

28 – Viz zejména rozsudky ze dne 10. prosince 2018, Wightman a další (C-621/18, EU:C:2018:999, bod 27), a ze dne 19. listopadu 2019, A. K. a další (Nezávislost kárného kolegia Nejvyššího soudu) (C-585/18, C-624/18 a C-625/18, EU:C:2019:982, bod 98).

29 – Viz čl. 94 odst. 1 a čl. 99 odst. 1 GDPR.

30 – Zdůrazňují, že v souladu s čl. 46 odst. 5 GDPR zůstávají rozhodnutí přijatá Komisí na základě čl. 26 odst. 4 směrnice 95/46 platná až do své změny, nahrazení nebo zrušení.

31 – Viz zejména rozsudky ze dne 7. února 1979, Francie v. Komise (15/76 a 16/76, EU:C:1979:29, bod 7); ze dne 17. května 2001, IECC v. Komise (C-449/98 P, EU:C:2001:275, bod 87), a ze dne 17. října 2013, Schaible (C-101/12, EU:C:2013:661, bod 50).

32 – Viz zejména rozsudky ze dne 16. dubna 2015, Parlament v. Rada (C-540/13, EU:C:2015:224, bod 35); ze dne 16. dubna 2015, Parlament v. Rada (C-317/13 a C-679/13, EU:C:2015:223, bod 45), a ze dne 22. září 2016, Parlament v. Rada (C-14/15 a C-116/15, EU:C:2016:715, bod 48).

33 – Zejména v rozsudku Schrems Soudní dvůr posoudil platnost rozhodnutí o „bezpečném přístavu“ z hlediska ustanovení Listiny, jejichž přijetí následovalo po přijetí tohoto rozhodnutí. Viz rovněž rozsudky ze dne 17. března 2011, AJD Tuna (C-221/09, EU:C:2011:153, bod 48), a ze dne 11. června 2015, Pfeifer & Langen (C-51/14, EU:C:2015:380, bod 42).

34 – Viz zejména rozsudky ze dne 15. července 2010, Pannon Gép Centrum (C-368/09, EU:C:2010:441, body 30 až 35); ze dne 10. února 2011, Andersson (C-30/10, EU:C:2011:66, body 20 a 21), jakož i ze dne 25. října 2018, Roche Lietuva (C-413/17, EU:C:2018:865, body 17 až 20).

35 – V tomto ohledu viz stanovisko generálního advokáta M. Bobka ve věci Fashion ID (C-40/17, EU:C:2018:1039, bod 87).

2. K předběžné povaze pochybností vyjádřených DPC

94. Podle německé vlády je žádost o rozhodnutí o předběžné otázce nepřijatelná z důvodu, že odvolací řízení, které je uvedeno v bodě 65 rozsudku Schrems, předpokládá, že orgán dozoru přijme konečné stanovisko k opodstatněnosti výtek vznesených stěžovatelem proti platnosti dotčeného rozhodnutí. Tak tomu v projednávané věci není, neboť DPC vyjádřil pochybnosti o platnosti rozhodnutí 2010/87, které M. Schrems ostatně nezpochybňuje, v návrhu rozhodnutí, který byl vydán předběžně, aniž tím bylo dotčeno případné podání doplňujících vyjádření ze strany společnosti Facebook Ireland a M. Schremse.

95. Domnívám se, že předběžná povaha pochybností vyjádřených DPC nemá vliv na přípustnost žádosti o rozhodnutí o předběžné otázce. Kritéria přípustnosti předběžné otázky je totiž třeba posuzovat ve vztahu k předmětu sporu, jak je vymezen předkládajícím soudem³⁶. Je přitom nesporné, že se týká platnosti rozhodnutí 2010/87. Podle předkládacího rozhodnutí a rozsudku k němu přiloženému se tento soud domníval, že pochybnosti vyjádřené DPC – aniž je důležité, zda byly předběžné nebo konečné – jsou opodstatněné, a proto se Soudního dvora dotázal na platnost tohoto rozhodnutí. Za těchto podmínek je objasnění Soudního dvora v tomto ohledu nepochybně relevantní k tomu, aby předkládající soud mohl rozhodnout o sporu, který mu byl předložen.

3. K nejistotě ohledně vymezení skutkového rámce

96. Vláda Spojeného království tvrdí, že skutkový rámec popsany předkládajícím soudem obsahuje několik mezer, které ohrožují přípustnost předběžných otázek. Tento soud neobjasnil, zda osobní údaje týkající se M. Schremse byly do Spojených států skutečně předány, ani, v případě kladné odpovědi, zda byly shromážděny americkými orgány. Ani právní základ pro tato případná předání nebyl s určitostí určen, jelikož předkládací rozhodnutí se omezuje na uvedení toho, že údaje evropských uživatelů sociální sítě Facebook jsou předávány „z velké části“ na základě standardních smluvních doložek stanovených v rozhodnutí 2010/87. V každém případě nebylo prokázáno, že smlouva mezi společností Facebook Ireland a Facebook Inc., dovoláváná na podporu sporného předávání, věrně přejímá tyto doložky. Německá vláda rovněž zpochybňuje přípustnost žádosti o rozhodnutí o předběžné otázce z důvodu, že předkládající soud nezkoumal, zda M. Schrems nepochybně udělil souhlas s předmětnými předáními, v kterémžto případě by tato předání byla platně založena na čl. 26 odst. 1 směrnice 95/46 [jehož obsah v podstatě přebírá čl. 49 odst. 1 písm. a) GDPR].

97. Tyto argumenty nijak nezpochybňují relevanci žádosti o rozhodnutí o předběžné otázce s ohledem na předmět sporu v původním řízení. Vzhledem k tomu, že tento spor má původ ve výkonu procesního prostředku, který je stanoven v bodě 65 rozsudku Schrems, ze strany DPC, je jeho samotným předmětem dosáhnout u vnitrostátního soudu předložení žádosti o rozhodnutí o předběžné otázce týkající se platnosti rozhodnutí 2010/87. Německá vláda a vláda Spojeného království ve skutečnosti popírají nezbytnost předběžných otázek nikoli pro určení, zda je toto rozhodnutí platné, ale k tomu, aby DPC mohl rozhodnout *in concreto* o stížnosti M. Schremse.

98. V každém případě i z hlediska tohoto řízení, které je podkladem pro spor v původním řízení, se mi předběžné otázky týkající se platnosti rozhodnutí 2010/87 nejeví jako irelevantní. Předkládající soud totiž prokázal, že společnost Facebook Ireland nadále předávala údaje svých uživatelů do Spojených států i po zrušení rozhodnutí o „bezpečném přístavu“ a že tato předávání jsou přinejmenším z části

36 – Viz bod 87 tohoto stanoviska.

založena na rozhodnutí 2010/87. Navíc, i když může být výhodné, aby všechny relevantní skutečnosti byly prokázány dříve, než předkládající soud vykoná svou pravomoc na základě článku 267 SFEU, pouze tomuto soudu přísluší, aby posoudil, v jaké fázi řízení potřebuje rozhodnutí Soudního dvora o předběžné otázce³⁷.

99. Vzhledem k výše uvedeným úvahám se domnívám, že žádost o rozhodnutí o předběžné otázce je přípustná.

C. K použitelnosti unijního práva na předávání osobních údajů za obchodními účely do třetího státu, který je může zpracovávat pro účely národní bezpečnosti (první otázka)

100. Podstatou první otázky předkládajícího soudu je, zda se unijní právo vztahuje na předávání osobních údajů společností, která je usazena v členském státě, společnosti usazené ve třetí zemi uskutečňované z obchodních důvodů, pokud takové údaje mohou být poté, co bylo předávání zahájeno, zpracovány veřejnými orgány této třetí země za účely, které zahrnují i ochranu národní bezpečnosti.

101. Význam této otázky pro řešení sporu v původním řízení spočívá v tom, že pokud by takové předávání spadalo mimo působnost unijního práva, byly by všechny námitky vznesené proti platnosti rozhodnutí 2010/87 v projednávané věci neopodstatněné.

102. Jak uvedl předkládající soud, zpracování osobních údajů, jež se týká národní bezpečnosti, bylo z působnosti směrnice 95/46 vyloučeno na základě jejího čl. 3 odst. 2. Nyní čl. 2 odst. 2 GDPR upřesňuje, že se toto nařízení nevztahuje na zpracování osobních údajů prováděné při výkonu činností, které nespádají do oblasti působnosti unijního práva, nebo příslušnými orgány za účelem ochrany před hrozbami pro veřejnou bezpečnost. Tato ustanovení odrážejí výhradu pravomoci, kterou čl. 4 odst. 2 SEU přiznává členským státům v oblasti ochrany národní bezpečnosti.

103. DPC, M. Schrems, Irsko, německá, rakouská, belgická, česká, nizozemská, polská a portugalská vláda, jakož i Parlament a Komise tvrdí, že na takové předávání, jako je předávání uvedené ve stížnosti M. Schremse, se tato ustanovení nevztahují, a proto spadá do působnosti unijního práva. Společnost Facebook Ireland zastává opačný názor. Ztotožňují se s prvně uvedeným názorem.

104. V tomto ohledu je třeba zdůraznit, že předávání osobních údajů z členského státu do třetí země představuje jako takové „zpracování“ ve smyslu čl. 4 bodu 2 GDPR prováděné na území členského státu³⁸. Předmětem první předběžné otázky je právě určit, zda se unijní právo vztahuje na *zpracování, kterým je samotné předávání*. Tato otázka se netýká použitelnosti unijního práva na případné následné zpracovávání údajů předaných do Spojených států americkými orgány pro účely národní bezpečnosti, které nespádá do místní působnosti GDPR³⁹.

37 – V tomto smyslu viz rozsudky ze dne 1. dubna 1982, Holdijk a další (141/81 až 143/81, EU:C:1982:122, bod 5), a ze dne 9. prosince 2003, Gasser (C-116/02, EU:C:2003:657, bod 27).

38 – V tomto smyslu viz rozsudek ze dne 30. května 2006, Parlament v. Rada a Komise (C-317/04 a C-318/04, EU:C:2006:346, dále jen „rozsudek PNR“, bod 56), jakož i rozsudek Schrems (bod 45). Článek 4 odst. 2 GDPR v podstatě přebírá definici pojmu „zpracování“, která byla obsažena v čl. 2 písm. b) směrnice 95/46.

39 – V souladu s čl. 3 odst. 1 GDPR se toto nařízení vztahuje na zpracování osobních údajů v souvislosti s činnostmi provozovny správce nebo zpracovatele v Unii bez ohledu na to, zda zpracování probíhá v Unii, či mimo ni. Otázku použitelnosti unijního práva na zpracování zpravodajskými službami třetí země mimo Unii je třeba odlišit od otázky relevance pravidel a zvyklostí při tomto zpracování v dotčené třetí zemi za účelem určení, zda v ní je zajištěna odpovídající úroveň ochrany. Tato poslední otázka je předmětem druhé předběžné otázky a bude posouzena v bodech 201 až 229 tohoto stanoviska.

105. Z tohoto hlediska je třeba pro účely určení, zda se unijní právo vztahuje na předávání dotčených údajů, zohlednit pouze činnost, v jejímž rámci dochází k tomuto předávání, aniž je relevantní účel případného následného zpracování předaných údajů veřejnými orgány třetí země určení⁴⁰.

106. Z předkládacího rozhodnutí přitom vyplývá, že předávání uvedené ve stížnosti M. Schremse je součástí obchodní činnosti. K tomuto předávání ostatně nedochází s cílem umožnit následné zpracování dotčených údajů americkými orgány pro účely národní bezpečnosti.

107. Přístup navržený společností Facebook Ireland by ostatně zbavil užitečného účinku ustanovení GDPR týkající se předávání do třetích zemí, jelikož nelze nikdy vyloučit, že údaje předávané v rámci obchodní činnosti budou po předání zpracovávány pro účely národní bezpečnosti.

108. Výklad, který zastávám, je potvrzen zněním čl. 45 odst. 2 písm. a) GDPR. Toto ustanovení uvádí, že pokud Komise přijímá rozhodnutí o odpovídající úrovni ochrany, vezme v úvahu zejména právní předpisy třetí země, které se týkají *národní bezpečnosti*. Z toho lze vyvodit, že možnost, že údaje budou zpracovány ze strany orgánů třetí země určené za účelem ochrany národní bezpečnosti, nečiní unijní právo nepoužitelným na zpracování představované předáním údajů do této třetí země.

109. Úvahy a závěry, které Soudní dvůr přijal v rozsudku ve věci Schrems, spočívají rovněž na tomto předpokladu. Soudní dvůr v něm zejména přezkoumal platnost rozhodnutí o „bezpečném přístavu“ v rozsahu, v němž se týká předávání osobních údajů do Spojených států, kde mohly být shromažďovány a zpracovávány pro účely ochrany národní bezpečnosti, s ohledem na čl. 25 odst. 6 směrnice 95/46 ve spojení s Listinou⁴¹.

110. S ohledem na tyto úvahy mám za to, že se unijní právo vztahuje na předávání osobních údajů z členského státu do třetí země, pokud je toto předávání součástí obchodní činnosti, aniž je relevantní, že předávané údaje mohou být zpracovány ze strany veřejných orgánů této třetí země za účelem ochrany národní bezpečnosti.

D. K úrovni ochrany vyžadované v rámci předávání založeného na standardních smluvních doložkách (první část šesté otázky)

111. První částí šesté otázky se předkládající soud táže, jaká je úroveň ochrany základních práv subjektů údajů, která musí být zajištěna proto, aby mohly být osobní údaje předávány do třetí země na základě standardních smluvních doložek uvedených v rozhodnutí 2010/87.

112. Uvedený soud zdůrazňuje, že v rozsudku Schrems vyložil Soudní dvůr čl. 25 odst. 6 směrnice 95/46 (jehož obsah je v podstatě převzat v čl. 45 odst. 3 GDPR) tak, že stanoví, že Komise může přijmout rozhodnutí o *odpovídající* úrovni ochrany pouze poté, co se ujistila, že třetí země, na kterou se vztahuje, zaručuje odpovídající úroveň ochrany, tak, že předpokládá, že tato země prokáže, že zajišťuje úroveň ochrany základních práv a svobod, která je v *zásadě rovnocenná* úrovni zaručené v rámci Unie na základě této směrnice vykládané ve světle Listiny⁴².

113. V tomto kontextu první část šesté předběžné otázky vyzývá Soudní dvůr k tomu, aby určil, zda použití „standardních smluvních doložek“ přijatých Komisí na základě čl. 26 odst. 4 směrnice 95/46 – které odpovídají „standardním doložkám o ochraně“ nyní uvedeným v čl. 46 odst. 2 písm. c) GDPR – musí umožnit dosažení úrovně ochrany odpovídající témuž standardu „podstatné rovnocennosti“.

40 – Ve svém stanovisku ve věci Ministerio Fiscal (C-207/16, EU:C:2018:300, bod 47) jsem zdůraznil rozlišení mezi jednak přímým zpracováním osobních údajů v rámci výkonu státní moci a jednak obchodním zpracováním s následným používáním veřejnými orgány.

41 – Stejným způsobem Soudní dvůr v posudku 1/15 (Dohoda PNR EU-Kanada) ze dne 26. července 2017 (EU:C:2017:592, dále jen „posudek 1/15“) přezkoumal slučitelnost návrhu mezinárodní dohody mezi Kanadou a Uníí o údajích, které měly být po předání do Kanady zpracovány veřejnými orgány pro účely ochrany národní bezpečnosti, s články 7, 8 a 47 Listiny.

42 – Rozsudek Schrems (bod 73). Soudní dvůr potvrdil tento závěr v posudku 1/15 (bod 134).

114. V tomto ohledu čl. 46 odst. 1 GDPR stanoví, že správce může předat osobní údaje do třetí země, „pouze pokud správce poskytl *vhodné záruky* a za podmínky, že jsou k dispozici vymahatelná práva subjektu údajů a účinná právní ochrana subjektů údajů“ (kurziva provedena autorem tohoto stanoviska)⁴³. Podle čl. 46 odst. 2 písm. c) GDPR mohou tyto záruky vyplývat zejména ze standardních doložek o ochraně vypracovaných Komisí.

115. Stejně jako DPC, M. Schrems a Irsko mám za to, že „odpovídající záruky“ poskytnuté správcem, na které odkazuje čl. 46 odst. 1 GDPR, musí zajistit, aby práva subjektů, jejichž údaje jsou předávány, požívala, tak jako v rámci předávání založeného na rozhodnutí o odpovídající úrovni ochrany, úroveň ochrany, která je v zásadě rovnocenná úrovni ochrany, která vyplývá z GDPR ve spojení s Listinou.

116. Tento závěr vyplývá z cíle tohoto ustanovení a z předpisu, jehož je součástí.

117. Cílem článků 45 a 46 GDPR je zajistit kontinuitu vysoké úrovně ochrany osobních údajů zajištěné tímto nařízením, jsou-li předávány mimo Unii. Článek 44 GDPR, nadepsaný „Obecná zásada pro předávání“, totiž zahajuje kapitolu V týkající se předávání osobních údajů do třetích zemí tím, že stanoví, že veškerá ustanovení této kapitoly se použijí s cílem zajistit, aby úroveň ochrany zaručená GDPR nebyla v případě předávání do třetího státu znehodnocena⁴⁴. Cílem tohoto pravidla je zabránit tomu, aby byly standardy ochrany vyplývající z unijního práva obcházeny předáváním osobních údajů do třetí země za účelem jejich zpracování⁴⁵. S ohledem na tento cíl nezáleží na tom, zda je předávání založeno na rozhodnutí o odpovídající úrovni ochrany, nebo na zárukách poskytnutých správcem, zejména prostřednictvím smluvních doložek. Požadavky na ochranu základních práv zaručených Listinou nečiní rozdíl v závislosti na právním základu, na němž dané předání spočívá⁴⁶.

118. Naproti tomu způsob, jakým je zachována kontinuita vysoké úrovně ochrany, se liší v závislosti na právním základu předávání.

119. Cílem rozhodnutí o odpovídající úrovni ochrany je konstatovat, že uvedená třetí země sama zajišťuje takovou úroveň ochrany, jako je úroveň ochrany, které musí být dosaženo v Unii. Přijetí rozhodnutí o odpovídající úrovni ochrany předpokládá, že Komise předem posoudí úroveň ochrany zaručenou právem a zvyklostmi určité třetí země ve světle faktorů stanovených v čl. 45 odst. 3 GDPR. Osobní údaje tedy mohou být předávány do uvedené třetí země, aniž správce musí získat zvláštní povolení.

120. Kromě toho, jak je podrobněji vysvětleno v následujícím oddíle, vhodné záruky nabízené správcem směřují k zajištění vysoké úrovně ochrany v případě nedostatečnosti záruk dostupných ve třetí zemi určení. I když čl. 46 odst. 1 GDPR umožňuje, aby byly osobní údaje předávány do třetích států, které nezajišťují odpovídající úroveň ochrany, toto ustanovení však takové předávání umožňuje pouze v případě, že jsou vhodné záruky poskytnuty jinými prostředky. Standardní smluvní doložky přijaté Komisí v tomto ohledu představují obecný mechanismus použitelný na předávání bez ohledu na třetí zemi určení a úroveň ochrany, která je v ní zajištěna.

43 – Článek 26 odst. 2 směrnice 95/46 stanovil, že členský stát může povolit takové předávání, „pokud správce poskytne *dostatečná ochranná opatření [dostatečné záruky]* pro ochranu soukromí a základních práv a svobod osob, jakož i pro výkon odpovídajících práv“ (kurzivou zvýraznil autor stanoviska stanoviska). Pojmy „dostatečné záruky“ a „vhodné záruky“ uvedené v tomto ustanovení a v čl. 46 odst. 1 GDPR mají podle mého názoru stejný obsah.

44 – V tomto ohledu bod 6 odůvodnění GDPR uvádí, že v rámci Unie i v případě předávání mimo Unii musí být zajištěna „vysoká úroveň“ ochrany údajů. Viz rovněž bod 101 odůvodnění GDPR.

45 – Viz rozsudek Schrems (bod 73) a posudek 1/15 (bod 214).

46 – To platí, aniž je dotčena možnost předávat osobní údaje i v případě neexistence vhodných záruk na základě důvodů pro výjimku stanovených v čl. 49 odst. 1 GDPR.

E. K platnosti rozhodnutí 2010/87 s ohledem na články 7, 8 a 47 Listiny (sedmá, osmá a jedenáctá otázka)

121. Podstatou sedmé otázky předkládajícího soudu je, zda je rozhodnutí 2010/87 neplatné z důvodu, že nezavazuje orgány třetích států, do kterých jsou předávány údaje na základě standardních smluvních doložek stanovených v příloze k tomuto rozhodnutí, a zejména že jim nebrání v tom, aby požadovaly od dovozce, aby jim tyto údaje poskytl. Tato otázka tedy zpochybňuje samotnou možnost zajistit odpovídající úroveň ochrany těchto údajů prostřednictvím mechanismů výlučně smluvní povahy. Jedenáctá otázka se týká obecně platnosti rozhodnutí 2010/87 s ohledem na články 7, 8 a 47 Listiny.

122. Osmá otázka vyzývá Soudní dvůr, aby určil, zda je orgán dozoru povinen využít pravomocí, které mu přiznává čl. 58 odst. 2 písm. f) a j) GDPR, k pozastavení předávání do třetí země na základě standardních smluvních doložek stanovených v rozhodnutí 2010/87, pokud má za to, že dovozce údajů v ní podléhá povinnostem, které mu brání v plnění těchto doložek a mají za následek, že není zajištěna odpovídající ochrana předaných údajů. Vzhledem k tomu, že odpověď na tuto otázku má podle mého názoru dopad na platnost rozhodnutí 2010/87⁴⁷, budu se jí zabývat společně se sedmou a jedenáctou otázkou.

123. Když znění čl. 46 odst. 1 GDPR stanoví, že „[j]estliže neexistuje rozhodnutí podle čl. 45 odst. 3, správce nebo zpracovatel mohou předat osobní údaje do třetí země [...], pouze pokud správce nebo zpracovatel poskytl vhodné záruky [...]“ (kurziva provedena autorem tohoto stanoviska), zdůrazňuje logiku, kterou mají takové smluvní mechanismy, jako je mechanismus stanovený v rozhodnutí 2010/87. Jak zdůrazňují body 108 a 114 odůvodnění GDPR, cílem těchto mechanismů je umožnit předávání do třetích zemí, pro které Komise nepřijala rozhodnutí o odpovídající úrovni ochrany, přičemž případné nedostatky ochrany zajištěné v právním řádu této třetí země jsou tedy vyrovnány zárukami, které se vývozce a dovozce údajů smluvně zaváží dodržovat.

124. Vzhledem k tomu, že důvod existence smluvních záruk spočívá právě ve zhojení možných mezer v ochraně poskytované třetími zeměmi určení, nemůže platnost rozhodnutí, v němž Komise konstatuje, že některé standardní doložky tyto mezery odpovídajícím způsobem vyplňují, záviset na úrovni ochrany zajištěné v každé z konkrétních třetích zemí, do kterých mohou být údaje předávány. Platnost takového rozhodnutí závisí pouze na pevnosti záruk, které stanoví tyto doložky s cílem vyrovnat případnou nedostatečnost ochrany ve třetí zemi určení. Efektivita těchto záruk musí být posuzována rovněž s ohledem na záruky představované pravomocemi orgánů dozoru na základě čl. 58 odst. 2 GDPR.

125. V tomto ohledu, jak v podstatě uvedli DPC, M. Schrems, BSA, Irsko, rakouská, francouzská, polská a portugalská vláda, jakož i Komise, záruky, které obsahují standardní smluvní doložky, mohou být oslabeny, ba dokonce zmařeny, jestliže právo třetí země určení ukládá dovozci údajů povinnosti, které jsou v rozporu s tím, co vyžadují tyto doložky. Právní kontext v třetí zemi určení tak může v závislosti na konkrétních okolnostech předávání⁴⁸ znemožňovat splnění povinností stanovených těmito doložkami.

126. Za těchto podmínek, jak zdůraznil M. Schrems a Komise, je smluvní mechanismus stanovený v čl. 46 odst. 2 písm. c) GDPR založen na odpovědnosti vývozce údajů, jakož i podpůrně, orgánů dozoru. V každém jednotlivém případě správce nebo, v případě jeho nečinnosti, orgán dozoru, přezkoumá, zda právo třetí země určení brání splnění standardních doložek, a tudíž i odpovídající ochraně předávaných údajů, takže je třeba předávání zakázat nebo pozastavit.

47 – Viz bod 128 tohoto stanoviska.

48 – Představme si například, že třetí země stanoví poskytovatelům telekomunikačních služeb povinnost umožnit veřejným orgánům přístup k předávaným údajům bez jakýchkoli omezení a záruk. Zatímco by takoví poskytovatelé nebyli schopni dodržet standardní smluvní doložky, podnikům, kterým není tato povinnost uložena, by v tom nic nebránilo.

127. Vzhledem k těmto vyjádřením se domnívám, že skutečnost, že rozhodnutí 2010/87 a standardní smluvní doložky, které stanoví, nejsou pro orgány třetí země určení závazné, sama o sobě nečiní toto rozhodnutí neplatné. Soulad rozhodnutí 2010/87 s články 7, 8 a 47 Listiny podle mého názoru závisí na tom, zda existují dostatečně pevné mechanismy, které umožňují zajistit, aby se předávání založené na standardních smluvních doložkách pozastavilo nebo bylo zakázáno v případě porušení těchto doložek nebo nemožnosti je splnit.

128. V tomto ohledu čl. 46 odst. 1 GDPR stanoví, že k předání založenému na vhodných zárukách může dojít pouze „za podmínky, že jsou k dispozici vymahatelná práva subjektu údajů a účinná právní ochrana“. Bude třeba ověřit, zda záruky stanovené v doložkách uvedených v příloze rozhodnutí 2010/87, které jsou doplněny pravomocemi orgánů dozoru, umožňují zajistit dodržení této podmínky. Podle mého názoru tomu tak je pouze tehdy, pokud existuje *povinnost* – správců (oddíl 1) a v případě jejich nečinnosti orgánů dozoru (oddíl 2) – pozastavit nebo zakázat předávání, pokud z důvodu rozporu mezi povinnostmi vyplývajících ze standardních doložek a povinnostmi uloženými právem třetí země určení nemohou být tyto doložky dodrženy.

1. K povinností správců

129. Zprv standardní smluvní doložky uvedené v příloze rozhodnutí 2010/87 vyžadují, aby v případě rozporu mezi povinnostmi, které stanoví, a požadavky vyplývajících z práva třetí země určení nebyly tyto doložky uplatňovány na podporu předávání do této třetí země nebo, pokud již bylo předávání zahájeno na základě uvedených doložek, byl vývozce údajů o tomto rozporu informován a mohl toto předávání zastavit.

130. Na základě doložky 5 písm. a) se dovozce zavazuje, že osobní údaje bude zpracovávat pouze jménem vývozce údajů a v souladu s jeho pokyny a se standardními smluvními doložkami. Nebude-li moci dovozce dodržování doložek zajistit, zavazuje se o tom neprodleně informovat vývozce údajů, který je v takovém případě oprávněn pozastavit předávání údajů nebo odstoupit od smlouvy⁴⁹.

131. Poznámka pod čarou 5 k doložce 5 stanoví, že standardní doložky nejsou porušeny, pokud dovozce údajů splní povinné požadavky vnitrostátních právních předpisů vztahujících se na dovozce údajů v třetí zemi, které nepřekračují rámec toho, co je nezbytné v demokratické společnosti, na základě jednoho ze zájmů uvedených v čl. 13 odst. 1 směrnice 95/46 (jehož obsah je v zásadě převzat v čl. 23 odst. 1 GDPR), mezi které patří i veřejná bezpečnost a bezpečnost státu. Naopak porušení těchto doložek za účelem dosažení souladu s kontradiktorní povinností vycházející z práva třetí země určení, která překračuje meze toho, co je přiměřené ochraně legitimního zájmu, který Unie uznává, se považuje za porušení uvedených doložek.

132. Podle mého názoru, jak tvrdili M. Schrems a Komise, doložku 5 písm. a) nelze vykládat tak, že znamená, že pozastavení předávání nebo odstoupení od smlouvy je pouze fakultativní, pokud dovozce není schopen dodržovat standardní doložky. I když tato doložka zmiňuje pouze právo vývozce údajů v tomto smyslu, musí být toto znění chápáno ve vztahu ke smluvnímu rámci, jehož je součástí. Skutečnost, že vývozce údajů má v rámci svých dvoustranných vztahů s dovozcem údajů právo pozastavit předávání nebo odstoupit od smlouvy, pokud se dovozce údajů nachází v neschopnosti dostát dotčeným doložkám, není na újmu povinnosti vývozce údajů postupovat tak s *ohledem na*

49 – Kromě toho poznamenávám, že doložka 5 písm. d) bod i) zbavuje dovozce údajů povinnosti oznámit vývozci údajů právně závazné požadavky na zveřejnění ze strany donucovacího orgánu třetí země, pokud takové oznámení právo této třetí země zakazuje. V takovém případě nebude mít vývozce údajů možnost pozastavit předávání, pokud toto zveřejnění, o kterém nebude vědět, porušuje standardní doložky. Na základě doložky 5 písm. a) je nicméně dovozce údajů povinen případně oznámit vývozci údajů skutečnost, že se domnívá, že právní předpisy této třetí země mu zakazují splnit jeho povinnosti na základě dohodnutých smluvních doložek.

požadavky na ochranu práv subjektů údajů vyplývající z GDPR. Jakýkoli jiný výklad by vedl k neplatnosti rozhodnutí 2010/87, jelikož smluvní doložky, které stanoví, by nedovolovaly opatřit předávání „vhodnými zárukami“, jak vyžaduje čl. 46 odst. 1 GDPR vykládaný ve světle ustanovení Listiny⁵⁰.

133. Navíc podle doložky 5 písm. b) dovozce údajů osvědčuje, že nemá důvod se domnívat, že mu právní předpisy, kterým podléhá, brání plnit pokyny vývozce údajů a jeho povinnosti vyplývající ze smlouvy. Pokud jsou tyto právní předpisy předmětem změny, která by mohla mít výrazně nepříznivý dopad na záruky a povinnosti stanovené standardními doložkami, oznámí dovozce údajů neprodleně tuto změnu vývozci údajů, který je v takovém případě oprávněn pozastavit předávání údajů nebo odstoupit od smlouvy. V souladu s doložkou 4 písm. g) předá vývozce oznámení obdržené od dovozce příslušnému orgánu dozoru, pokud se vývozce rozhodne pokračovat v předávání.

134. Považuji za nezbytné zde uvést několik upřesnění týkajících se obsahu přezkumu, který musí strany smlouvy provést s ohledem na poznámku pod čarou k doložce 5 za účelem určení, zda povinnosti, které právo třetího státu ukládá dovozci, s sebou nesou porušení standardních doložek, a tudíž brání, aby bylo předávání doplněno vhodnými zárukami. Tato problematika byla v podstatě vznesena v rámci druhé části šesté předběžné otázky.

135. Takový přezkum podle mého názoru vyžaduje zohlednění všech okolností charakterizujících každé předávání, mezi které patří i povaha údajů a jejich případná citlivá povaha, mechanismy zavedené vývozcem nebo dovozcem údajů za účelem zajištění jejich bezpečnosti⁵¹, povaha a účel zpracování ze strany veřejných orgánů třetí země, jehož předmětem údaje budou, podmínky tohoto zpracování, jakož i omezení a záruky poskytované touto třetí zemí. Mám za to, že prvky charakterizující činnosti zpracování veřejnými orgány a záruky použitelné v právním řádu uvedené třetí země se mohou překrývat s těmi, které jsou uvedeny v čl. 45 odst. 2 GDPR.

136. Zadržím standardní smluvní doložky uvedené v příloze rozhodnutí 2010/87 zavádějí ve prospěch subjektů údajů vymahatelná práva a účinnou právní ochranu proti vývozci a podpůrně proti dovozci údajů.

137. Doložka 3, nadepsaná „Doložka ve prospěch třetí strany“, v odstavci 1 stanoví právo subjektu údajů podat žalobu proti vývozci údajů v případě porušení zejména doložky 5 písm. a) nebo b). V souladu s doložkou 3 odst. 2 v případech, kdy vývozce údajů fakticky zmizel nebo kdy z právního hlediska zanikl, je subjekt údajů oprávněn tuto doložku uplatnit proti dovozci údajů.

138. Doložka 6 odst. 1 poskytuje jakémukoli subjektu údajů, který utrpěl v důsledku porušení povinností uvedených v doložce 3 škodu, právo obdržet od vývozce údajů za utrpěnou škodu náhradu. Na základě doložky 7 odst. 1 se dovozce údajů zavazuje, že uplatní-li proti němu subjekt údajů práva ve prospěch třetí strany nebo uplatní-li nárok na náhradu škody, přistoupí dovozce údajů na rozhodnutí subjektu údajů předat spor k mediaci prováděné nezávislou osobou nebo popřípadě orgánem dozoru či předat spor soudům v členském státě, ve kterém je vývozce údajů usazen.

50 – Z judikatury vyplývá, že ustanovení prováděcího aktu musí být vykládána v souladu s ustanoveními základního aktu, kterým normotvůrce povolil jeho přijetí [v tomto smyslu viz zejména rozsudky ze dne 26. července 2017, Česká republika v. Komise (C-696/15 P, EU:C:2017:595, bod 51); ze dne 17. května 2018, Evonik Degussa (C-229/17, EU:C:2018:323, bod 29), a ze dne 20. června 2019, ExxonMobil Production Deutschland (C-682/17, EU:C:2019:518, bod 112)]. Mimoto musí být unijní akt vykládán v co největším možném rozsahu způsobem, který nezpochybní jeho platnost, a v souladu s veškerým primárním právem, mimo jiné i s ustanoveními Listiny [viz zejména rozsudek ze dne 14. května 2019, M a další (Odnětí postavení uprchlíka) (C-391/16, C-77/17 a C-78/17, EU:C:2019:403, bod 77 a citovaná judikatura)].

51 – V tomto ohledu bod 109 odůvodnění GDPR vybízí vývozce a dovozce údajů k poskytování dalších záruk zejména prostřednictvím smluvních závazků, které doplní standardní doložky o ochraně údajů.

139. Vedle procesních prostředků, které mají k dispozici na základě standardních smluvních doložek stanovených v příloze rozhodnutí 2010/87, mohou subjekty údajů, pokud se domnívají, že tyto doložky byly porušeny, požádat orgány dozoru o přijetí nápravných opatření na základě čl. 58 odst. 2 GDPR, na něž odkazuje článek 4 rozhodnutí 2010/87⁵².

2. K povinností orgánů dozoru

140. Z následujících důvodů vyvozují, stejně jako M. Schrems, Irsko, německá, rakouská, nizozemská a portugalská vláda, jakož i EDPB, že čl. 58 odst. 2 GDPR ukládá orgánům dozoru, pokud po provedení pečlivého přezkumu mají za to, že údaje předávané do třetí země nepožívají odpovídající ochrany z důvodu nedodržení dohodnutých smluvních doložek, přijmout vhodná opatření k nápravě této protiprávnosti, a pokud je to nezbytné, nařídit pozastavení předávání.

141. Zaprvé podotýkám, že na rozdíl od toho, co tvrdí DPC, žádné ustanovení rozhodnutí 2010/87 neomezuje výkon pravomocí „uložit dočasné nebo trvalé omezení zpracování, včetně jeho zákazu“, a „nařídit přerušování toků údajů příjemci ve třetí zemi nebo toků údajů mezinárodní organizaci“, které mají orgány dozoru na základě čl. 58 odst. 2 písm. f) a j) GDPR, na výjimečné případy.

142. Původní znění článku 4 rozhodnutí 2010/87 sice v odstavci 1 omezilo výkon pravomocí orgánů dozoru pozastavit nebo zakázat přeshraniční toky údajů na určité případy, kdy je prokázáno, že předávání založené na smluvních podmínkách může mít závažné negativní důsledky pro záruky určené k ochraně subjektu údajů. Nicméně článek 4 tohoto rozhodnutí, pozměněný Komisí v roce 2016 za účelem dosažení souladu s rozsudkem Schrems⁵³, se nyní omezuje na odkázání na tyto pravomoci, aniž by je jakkoli omezoval. V každém případě prováděcí rozhodnutí Komise, jako je rozhodnutí 2010/87, nemůže platně omezit pravomoci svěřené orgánům dozoru na základě samotného GDPR⁵⁴.

143. Tento závěr není zpochybněn bodem 11 odůvodnění rozhodnutí 2010/87, který stanoví, že pravomoc pozastavit a zakázat předávání údajů lze uplatnit pouze „ve výjimečných případech“. Tento bod odůvodnění, který byl již obsažen v původní verzi tohoto rozhodnutí, se vztahoval k bývalému čl. 4 odst. 1 uvedeného rozhodnutí, který omezoval pravomoci orgánů dozoru. Při změně rozhodnutí 2010/87 rozhodnutím 2016/2297 Komise nezrušila, ani nezměnila uvedený bod odůvodnění za účelem jeho přizpůsobení obsahu znění nového článku 4. Bod 5 odůvodnění rozhodnutí 2016/2297 přesto znovu potvrdil pravomoc orgánů dozoru pozastavit nebo zakázat jakékoli předávání, které považují za odporující unijnímu právu, zejména z důvodu nedodržení standardních smluvních doložek dovozem údajů. Bod 11 odůvodnění rozhodnutí 2010/87 je tím, že nyní odporuje znění i cíli právně závazného ustanovení tohoto rozhodnutí, třeba kvalifikovat jako obsoletní⁵⁵.

144. Zadržím na rozdíl od toho, co rovněž tvrdí DPC, výkon pravomocí v oblasti pozastavení a zákazu stanovených v čl. 58 odst. 2 písm. f) a j) GDPR nepředstavuje ani pouhou možnost ponechanou na uvážení orgánů dozoru. Tento závěr podle mého názoru vyplývá z výkladu čl. 58 odst. 2 GDPR ve světle ostatních ustanovení tohoto nařízení a Listiny, jakož i z obecné systematiky a cílů rozhodnutí 2010/87.

52 – I když čl. 4 odst. 1 rozhodnutí 2010/87 odkazuje na čl. 28 odst. 3 směrnice 95/46, připomínám, že na základě čl. 94 odst. 2 GDPR se odkazy na tuto směrnici považují za odkazy na odpovídající ustanovení GDPR.

53 – Viz body 6 a 7 odůvodnění rozhodnutí 2016/2297. V bodech 101 až 104 rozsudku Schrems Soudní dvůr prohlásil za neplatné ustanovení rozhodnutí o „bezpečném přístavu“, které omezovalo pravomoci svěřené orgánům dozoru článkem 28 směrnice 95/46 na „výjimečné případy“, z důvodu, že Komise nebyla k omezení těchto pravomocí příslušná.

54 – Viz rozsudek Schrems (bod 103).

55 – V každém případě body odůvodnění unijního aktu nemají právní závaznost a nemohou být uplatňovány jako důvod pro odchýlení se od vlastních ustanovení dotčeného aktu. Viz rozsudky ze dne 19. listopadu 1998, Nilsson a další (C-162/97, EU:C:1998:554, bod 54); ze dne 12. května 2005, Meta Fackler (C-444/03, EU:C:2005:288, bod 25), a ze dne 10. ledna 2006, IATA a ELFAA (C-344/04, EU:C:2006:10, bod 76).

145. Zejména čl. 58 odst. 2 GDPR musí být vykládán ve světle čl. 8 odst. 3 Listiny a čl. 16 odst. 2 SFEU. V souladu s těmito ustanoveními dodržování požadavků, které s sebou nese základní právo na ochranu osobních údajů, podléhá kontrole nezávislých orgánů. Tento úkol dozoru nad dodržováním požadavků týkajících se ochrany osobních údajů, uvedený rovněž v čl. 57 odst. 1 písm. a) GDPR, implikuje povinnost orgánů dozoru jednat takovým způsobem, aby zajistily správné provádění tohoto nařízení.

146. Orgán dozoru tak musí s veškerou požadovanou péčí přezkoumat stížnost podanou subjektem, jehož údaje jsou údajně předávány do třetího státu v rozporu se standardními smluvními doložkami použitelnými na předávání⁵⁶. Článek 58 odst. 1 GDPR svěruje za tímto účelem orgánům dozoru značné vyšetřovací pravomoci⁵⁷.

147. Příslušný orgán dozoru je rovněž povinen náležitě reagovat na případná porušení práv subjektu údajů, která konstatuje na závěr šetření. V tomto ohledu má každý orgán dozoru na základě čl. 58 odst. 2 GDPR širokou škálu prostředků – různé pravomoci přijímat nápravná opatření vyjmenované v tomto ustanovení – k plnění úkolu, který mu byl svěřen⁵⁸.

148. I když volba nejúčinnějšího prostředku spadá do uvážení příslušného orgánu dozoru s ohledem na všechny okolnosti dotčeného předávání, je tento orgán povinen plně splnit svůj úkol dozoru, který mu byl svěřen. Tento orgán případně musí pozastavit předávání, pokud dospěje k závěru, že nejsou dodržovány standardní smluvní doložky a vhodná ochrana předávaných údajů nemůže být zajištěna jinými prostředky, ledaže by předávání ukončil sám vývozce.

149. Tento výklad je podpořen čl. 58 odst. 4 GDPR který stanoví, že výkon pravomocí svěřených tímto článkem orgánu dozoru podléhá vhodným zárukám, včetně účinné soudní ochrany a spravedlivého procesu, v souladu s článkem 47 Listiny. Článek 78 odst. 1 a 2 GDPR kromě toho uznává právo každé osoby na účinnou soudní ochranu proti právně závaznému rozhodnutí orgánu dozoru, které se jí týká, nebo pokud se tento orgán nezabývá její stížností⁵⁹.

150. Tato ustanovení znamenají, jak v podstatě tvrdí M. Schrems, BSA, Irsko, polská vláda a vláda Spojeného království, jakož i Komise, že rozhodnutí, kterým orgán dozoru nezakáže nebo nepozastaví předávání do třetí země na žádost osoby, která se dovolává nebezpečí, že údaje, které se jí týkají, tam budou zpracovávány v rozporu s jejími základními právy, může být předmětem žaloby. Uznání práva na účinnou soudní ochranu přitom předpokládá existence vázané, a nikoli čistě diskreční pravomoci orgánů dozoru. Kromě toho M. Schrems a Komise správně zdůraznili, že výkon účinného soudního přezkumu znamená, že orgán, který je autorem napadeného aktu, musí tento akt řádně odůvodnit⁶⁰. Tato povinnost uvést odůvodnění se podle mého názoru vztahuje na volbu orgánů dozoru využít některou z pravomocí, kterou jim svěruje čl. 58 odst. 2 GDPR.

151. Nicméně je třeba ještě odpovědět na argumenty, kterými DPC tvrdí, že i kdyby byly orgány dozoru povinny pozastavit nebo zakázat předávání, pokud to vyžaduje ochrana práv subjektu údajů, nebyla by tím přesto zajištěna platnost rozhodnutí 2010/87.

56 – Obdobně viz rozsudek Schrems (bod 63).

57 – Dodávám, že na základě doložky 8 odst. 2, která je obsažena v příloze rozhodnutí 2010/87, smluvní strany souhlasí s tím, že orgán dozoru má právo provést přezkoumání u dovozce údajů, které bude podléhat stejným podmínkám jako přezkoumání u vývozce údajů uskutečněné v souladu s rozhodným právem.

58 – V tomto smyslu viz rozsudek Schrems (bod 43).

59 – Podle bodu 141 odůvodnění GDPR musí mít každý subjekt údajů právo na účinnou soudní ochranu v souladu s článkem 47 Listiny, pokud orgán dozoru „nekoná, přestože je to nutné z důvodu ochrany práv [tohoto subjektu]“. Viz rovněž body 129 a 143 odůvodnění GDPR.

60 – Viz zejména rozsudky ze dne 28. července 2011, Samba Diouf (C-69/10, EU:C:2011:524, bod 57), a ze dne 17. listopadu 2011, Gajdarov (C-430/10, EU:C:2011:749, bod 41).

152. Zprv se DPC domnívá, že tato povinnost nenapravuje systémové problémy týkající se neexistence vhodných záruk v takové třetí zemi, jakou jsou Spojené státy. Pravomoci orgánů dozoru totiž mohou být vykonávány pouze případ od případu, i když mají mezery charakterizující americké právo obecnou a strukturální povahu. Z toho vyplývá nebezpečí, že jednotlivé orgány dozoru přijmou rozdílná rozhodnutí týkající se srovnatelných předávání.

153. V tomto ohledu nelze nezhlednit praktické obtíže spojené s legislativní volbou, aby orgány dozoru nesly odpovědnost za dozor nad dodržováním základních práv subjektů údajů v rámci konkrétního předávání nebo toků vůči konkrétnímu adresátovi. Tyto obtíže však podle mého názoru nezpůsobují neplatnost rozhodnutí 2010/87.

154. Unijní právo totiž podle mého názoru nevyžaduje, aby bylo stanoveno celkové a preventivní řešení pro všechna předávání do určité třetí země, která by s sebou mohla nést stejná rizika porušení základních práv.

155. Navíc riziko fragmentace přístupů jednotlivých orgánů dozoru je inherentní architektuře decentralizovaného dozoru, kterou normotvůrce zamýšlel⁶¹. Ostatně, jak zdůraznila německá vláda, kapitola VII GDPR, nadepsaná „Spolupráce a jednotnost“, zavádí mechanismy určené k zabránění tomuto riziku. Článek 60 tohoto nařízení stanoví v případě přeshraničního zpracování údajů postup spolupráce mezi dotčenými orgány dozoru a orgánem dozoru místa usazení správce, zvaným „vedoucí orgán dozoru“⁶². V případě rozdílných stanovisek musí spor rozhodnout EDPB⁶³. Tento sbor je na žádost orgánu dozoru rovněž příslušný k vydání stanovisek k jakékoli otázce s účinky ve více než jednom členském státě⁶⁴.

156. Zadruhé DPC namítá neplatnost rozhodnutí 2010/87 s ohledem na článek 47 Listiny z důvodu, že orgány dozoru mohou chránit práva subjektů údajů pouze do budoucna, aniž poskytují řešení těm, jejichž údaje již byly předány. DPC zejména uvádí, že čl. 58 odst. 2 GDPR nestanoví právo na přístup, opravu a výmaz údajů shromážděných veřejnými orgány třetí země, ani možnost nahradit škodu utrpěnou subjekty údajů.

157. Pokud jde o tvrzenou neexistenci práva na přístup, opravu a výmaz shromážděných údajů, je třeba konstatovat, že pokud ve třetí zemi určení neexistuje žádný účinný opravný prostředek, neumožní v rámci Unie stanovené opravné prostředky proti správci získat od veřejných orgánů této třetí země přístup k těmto údajům či jejich opravu nebo výmaz.

158. Domnívám se, že tato námitka nicméně neodůvodňuje neslučitelnost rozhodnutí 2010/87 s článkem 47 Listiny. Platnost tohoto rozhodnutí totiž nezávisí na úrovni ochrany existující v každé třetí zemi, do které mohou být údaje předány na základě standardních smluvních doložek, které stanoví. Pokud právo třetího státu určení brání dovozci v dodržení těchto doložek tím, že vyžaduje, aby veřejným orgánům poskytl přístup k údajům, který není spojen s vhodnými možnými opravnými prostředky, je v případě, že vývozce nepozastavil předávání podle doložky 5 písm. a) nebo b) uvedené v příloze rozhodnutí 2010/87, na orgánech dozoru, aby přijaly nápravná opatření.

159. Kromě toho, jak zdůraznil M. Schrems, subjekty, jejichž práva byla porušena, mají nyní na základě článku 82 GDPR právo na náhradu majetkové i nemajetkové újmy způsobené porušením tohoto nařízení od správce nebo zpracovatele⁶⁵.

61 – V tomto ohledu viz rozsudek ze dne 5. června 2018, Wirtschaftsakademie Schleswig-Holstein (C-210/16, EU:C:2018:388, body 69 až 73).

62 – Viz čl. 56 odst. 1 GDPR. V souladu s článkem 61 tohoto nařízení jsou orgány dozoru povinny si poskytovat vzájemnou pomoc. Článek 62 uvedeného nařízení jim umožňuje provádět společné postupy.

63 – Viz článek 65 GDPR.

64 – Viz čl. 64 odst. 2 GDPR.

65 – Článek 83 odst. 5 písm. c) GDPR stanoví rovněž pokuty správci v případě porušení článků 44 až 49 tohoto nařízení.

160. Jak vyplývá ze všech těchto úvah, má analýza neprokázala nic, co by mohlo ovlivnit platnost rozhodnutí 2010/87 s ohledem na články 7, 8 a 47 Listiny.

F. K neexistenci nutnosti odpovědět na ostatní předběžné otázky a přezkoumat platnost rozhodnutí o štítu na ochranu soukromí

161. V tomto oddíle uvedu důvody, které spočívají především v omezení předmětu sporu v původním řízení na platnost rozhodnutí 2010/87, na základě kterých se domnívám, že není třeba odpovídat na druhou až pátou, jakož i devátou a desátou předběžnou otázku ani se vyjádřit k platnosti rozhodnutí o štítu na ochranu soukromí.

162. Druhá předběžná otázka se týká určení standardů ochrany, které musí třetí země dodržovat, aby do ní mohly být údaje legálně předávány na základě standardních smluvních doložek, pokud tyto údaje mohou být po jejich předání zpracovány orgány této třetí země pro účely národní bezpečnosti. Třetí otázka předložená Soudnímu dvoru se týká určení prvků charakterizujících režim ochrany použitelný ve třetím státě určení, které je třeba zohlednit za účelem ověření, zda tyto standardy splňuje.

163. Podstatou čtvrté, páté a desáté otázky předkládajícího soudu je to, zda s ohledem na skutečnosti, které prokázal v souvislosti s právem Spojených států, jsou v něm stanoveny vhodné záruky proti zásahům do výkonu základních práv na dodržování soukromí, ochranu osobních údajů a účinnou soudní ochranu ze strany amerických zpravodajských orgánů.

164. Devátá předběžná otázka se týká vlivu, který má v rámci přezkumu, jímž orgán dozoru ověřuje, zda je předávání do Spojených států na základě standardních smluvních doložek, které jsou stanoveny v rozhodnutí 2010/87, spojeno s vhodnými zárukami, okolnost, že Komise v rozhodnutí o štítu na ochranu soukromí konstatovala, že Spojené státy poskytují odpovídající úroveň ochrany základních práv subjektů údajů před takovými zásahy.

165. Otázka platnosti rozhodnutí o štítu na ochranu soukromí nebyla předkládajícím soudem výslovně položena – i když, jak vysvětlím dále⁶⁶, čtvrtá, pátá a desátá předběžná otázka nepřímou zpochybňují opodstatněnost konstatování o odpovídající ochraně, které v tomto rozhodnutí Komise učinila.

166. Podle mého názoru s přihlédnutím ke skutečnostem, které vyplývají z výše uvedené analýzy, nemůže objasnění Soudního dvora ohledně těchto otázek ovlivnit jeho závěr týkající se platnosti *in abstracto* rozhodnutí 2010/87, ani tudíž ovlivnit řešení sporu v původním řízení (oddíl 1). Kromě toho i když se odpovědi Soudního dvora na uvedené otázky mohou v pozdější fázi ukázat jako užitečné pro DPC za účelem určení, zda v rámci řízení, na kterém je tento spor založen, musí být dotčené předávání *in concreto* pozastaveno z důvodu údajné neexistence vhodných záruk, je podle mého názoru předčasné tyto otázky rozhodnout v rámci projednávané věci (oddíl 2).

1. K neexistenci nutnosti odpovědi Soudního dvora s ohledem na předmět sporu v původním řízení

167. Připomínám, že spor v původním řízení vyplývá z toho, že DPC využil opravný prostředek popsáný v bodě 65 rozsudku Schrems, podle kterého musí každý členský stát umožnit orgánu dozoru, pokud to považuje za nezbytné pro účely projednání stížnosti, která mu byla předložena, požádat vnitrostátní soud, aby za tímto účelem předložil Soudnímu dvoru předběžnou otázku týkající se platnosti rozhodnutí o odpovídající úrovni ochrany – nebo *per analogiam* rozhodnutí o standardních smluvních doložkách.

⁶⁶ – Viz bod 175 tohoto stanoviska.

168. V tomto ohledu High Court (Vrchní soud) zdůraznil, že když mu DPC věc předložil, měl pouze možnost podat žádost o rozhodnutí o předběžné otázce týkající se platnosti rozhodnutí 2010/87, o kterou požádal DPC, v případě, že by sdílel jeho pochybnosti ohledně platnosti tohoto rozhodnutí, nebo v opačném případě jeho požadavek zamítnout. Uvedený soud se domnívá, že pokud by zvolil tuto druhou cestu, musel by žalobu zamítnout v plném rozsahu, neboť stížnost DPC neměla jiný předmět⁶⁷.

169. Supreme Court (Nejvyšší soud), k němuž společnost Facebook Ireland podala odvolání proti předkládacímu rozhodnutí, ve stejném smyslu popsal spor v původním řízení jako deklaratorní řízení, kterým DPC žádal předkládající soud, aby položil Soudnímu dvoru předběžnou otázku týkající se platnosti rozhodnutí 2010/87. Podle irského nejvyššího soudu byla tedy jedinou podstatnou otázkou vznesenou před předkládajícím soudem a Soudním dvorem otázka platnosti tohoto rozhodnutí⁶⁸.

170. S ohledem na takto vymezený předmět sporu v původním řízení předkládající soud položil Soudnímu dvoru svých prvních deset otázek, jelikož měl za to, že jejich přezkum bude součástí celkového posouzení, které je pro Soudní dvůr nezbytné, aby se v odpovědi na jedenáctou otázku vyjádřil k platnosti rozhodnutí 2010/87 z hlediska článků 7, 8 a 47 Listiny. Tato otázka představuje podle předkládacího rozhodnutí logické vyústění otázek, které jí předcházejí.

171. Z tohoto hlediska se domnívám, že druhá až pátá, jakož i devátá a desátá otázka vychází z předpokladu, že platnost rozhodnutí 2010/87 závisí na úrovni ochrany základních práv, která je stanovena v každém třetím státě, do kterého mohou být údaje předávány na základě standardních smluvních doložek, které stanoví. Jak přitom vyplývá z mé analýzy sedmé otázky⁶⁹, domnívám se, že je tento předpoklad chybný. O přezkum práva třetí země určení se jedná pouze tehdy, pokud Komise přijme rozhodnutí o odpovídající úrovni ochrany, nebo pokud správce – nebo případně příslušný orgán dozoru – ověřuje, zda v rámci předávání založeného na vhodných zárukách ve smyslu čl. 46 odst. 1 GDPR povinnosti, které právo této třetí země ukládá dovozci údajů, neohrožují účinnost ochrany zajištěné těmito zárukami.

172. V důsledku toho nemohou odpovědi Soudního dvora na výše uvedené otázky ovlivnit jeho závěr k jedenácté otázce⁷⁰. Proto není třeba na tuto otázku odpovídat z hlediska předmětu sporu v původním řízení.

173. Navrhuji Soudnímu dvoru, aby se omezil na projednání projednávané věci z hlediska předmětu tohoto sporu. Soudní dvůr by podle mého názoru neměl překročit meze toho, co vyžaduje řešení uvedeného sporu, tím, že se bude zabývat předběžnými otázkami z hlediska řízení, které je podkladem pro řízení probíhající před DPC. Jak bude uvedeno dále, tento návrh na zdrženlivost vychází jednak ze snahy nenarušit obvyklý průběh řízení, které bude muset pokračovat u DPC poté, co Soudní dvůr rozhodne o platnosti rozhodnutí 2010/87. Kromě toho s přihlédnutím ke skutkovým okolnostem projednávané věci považuji za poněkud předčasné, i z hlediska významu tohoto řízení, aby Soudní dvůr zkoumal problematiku nastolenou druhou až pátou, jakož i devátou a desátou otázkou.

67 – Rozsudek High Court (Vrchní soud) ze dne 3. října 2017 (bod 337).

68 – Podle rozsudku Supreme Court (Nejvyšší soud) ze dne 31. května 2019 (bod 2.7), „[t]he sole relief claimed by the DPC is, in substance, a reference to the CJEU under Article 267 [TFUE]“. Bod 2.9 tohoto rozsudku pokračuje: „Here, the only issue of substance which arises before either the Irish courts or the CJEU is the question of the validity or otherwise of Union measures. Whatever the view taken by the CJEU on that issue, *the Irish courts will have no further role, for the measures under question will either be found to be valid or invalid and in either event, that will be the end of the matter*“ (kurzivou zvýraznil autor stanoviska).

69 – Viz bod 124 tohoto stanoviska.

70 – Ze stejného důvodu Supreme Court (Nejvyšší soud) ve svém rozsudku ze dne 31. května 2019 (body 8.1 až 8.5) uznal, že není příslušný ke zpochybnění rozhodnutí předkládacího soudu předložit Soudnímu dvoru předběžné otázky a ke změně jejich znění, když současně vyjádřil pochybnosti ohledně nutnosti některých z těchto otázek. Zejména bod 8.5 uvedeného rozsudku stanoví: „The sole purpose of the proceedings before the courts in Ireland was to enable the High Court to refer that question of validity to the CJEU and obtain a definitive answer from the only court which has competence to make the decision in question. It is difficult, therefore, to see how the High Court needs answers to many of the questions which have been referred, for the answers to those questions are only relevant to the question of the validity of the challenged measures [...]“.

2. K důvodům, které svědčí v neprospěch přezkumu Soudního dvora s ohledem na předmět řízení probíhajícího u DPC

174. Ve své stížnosti podané k DPC se M. Schrems domáhá, aby tento orgán dozoru vykonal pravomoci, kterými disponuje na základě čl. 58 odst. 2 písm. f) GDPR, a nařídil společnosti Facebook Ireland, aby pozastavila předávání osobních údajů, které se ho týkají, do Spojených států prováděné na základě smluvních doložek. Na podporu tohoto návrhu se M. Schrems především dovolává toho, že tyto smluvní záruky nejsou vhodné ve vztahu k zásahům do výkonu jeho základních práv vyplývajících z činností amerických zpravodajských služeb.

175. Argumentace M. Schremse zpochybňuje zjištění, které Komise uvedla v rozhodnutí o štítu na ochranu soukromí, podle něhož Spojené státy zajišťují odpovídající úroveň ochrany údajů předávaných na základě tohoto rozhodnutí s ohledem na omezení přístupu k těmto údajům a jejich využívání americkými zpravodajskými orgány, jakož i právní ochraně, která je poskytována subjektům údajů⁷¹. Obavy vyjádřené předběžně⁷² DPC, jakož i předkládajícím soudem v rámci jeho čtvrté, páté a desáté otázky rovněž nepřímo zpochybňují opodstatněnost tohoto zjištění.

176. Rozhodnutí o štítu na ochranu soukromí se zajisté omezuje na konstatování, že úroveň ochrany osobních údajů předávaných podnikem usazenému ve Spojených státech, který autocertifikoval (sám osvědčil) přijetí těchto zásad⁷³, je odpovídající v souladu se zásadami, které stanoví. Úvahy v něm obsažené však překračují kontext předávání, na které se vztahuje toto rozhodnutí, jelikož se týkají práva a zvyklostí platných v této třetí zemi ohledně zpracování předávaných údajů za účelem ochrany národní bezpečnosti. Jak v podstatě uvedli společnost Facebook Ireland, M. Schrems, vláda Spojených států a Komise, dozor vykonávaný americkými zpravodajskými orgány, jakož i záruky proti riziku zneužití, které zahrnuje, a mechanismy směřující ke kontrole jejich dodržování se uplatní bez ohledu na právní základ dovolávaný na podporu předávání z hlediska unijního práva.

177. V tomto ohledu může být pro účely projednání stížnosti M. Schremse ze strany DPC relevantní otázka, zda jsou zjištění uvedená v tomto ohledu v rozhodnutí o štítu na ochranu soukromí závazná pro orgány dozoru, když přezkoumávají legalitu předávání prováděného na základě standardních smluvních doložek. V případě kladné odpovědi na tuto otázku vyvstane otázka, zda je toto rozhodnutí skutečně platné.

178. Nicméně nedoporučuji Soudnímu dvoru, aby o těchto otázkách rozhodl s jediným cílem pomoci DPC projednat tuto stížnost, i když na ně není třeba odpovídat proto, aby bylo předkládajícímu soudu umožněno vyřešit spor v původním řízení. Vzhledem k tomu, že řízení upravené v článku 267 SFEU zavádí dialog mezi soudy, nemá Soudní dvůr poskytovat objasnění za jediným účelem pomoci správnímu orgánu v rámci řízení, které je podkladem pro tento spor.

179. Výhrada se podle mého názoru uplatní tím spíše, že mu nebyla výslovně předložena otázka platnosti rozhodnutí o štítu na ochranu soukromí – přičemž kromě toho je toto rozhodnutí již předmětem žaloby na neplatnost projednávané před Tribunálem Evropské unie⁷⁴.

71 – Viz body 64 až 141 odůvodnění rozhodnutí o štítu na ochranu soukromí. Připomínám, že z čl. 1 odst. 2 tohoto rozhodnutí vyplývá, že štít na ochranu soukromí se skládá nejen ze zásad, k jejichž dodržování se musí zavázat podniky, které hodlají předávat údaje na základě uvedeného rozhodnutí, ale rovněž z prohlášení a oficiálních závazků získaných od vlády Spojených států, které jsou obsaženy v dokumentech, které jsou k rozhodnutí přiloženy.

72 – Návrh rozhodnutí DPC předchází přijetí rozhodnutí o štítu na ochranu soukromí. Jak DPC v tomto návrhu upřesnil, i když v něm předběžně došel k závěru, že záruky stanovené právem Spojených států neumožňují přinejmenším zajistit soulad předávání do této třetí země s článkem 47 Listiny, *nepřezkoumal, ani nezohlednil v této fázi nová ujednání plánovaná v návrhu dohody týkající se „štítu ochrany“, jelikož tato dohoda nebyla ještě přijata*. V bodě 307 svého rozsudku ze dne 3. října 2017 však High Court (Vrchní soud) uvádí: „It is fair to conclude [...] that the decision of the Commission in regard to the adequacy of the protections afforded to EU citizens against interference by the intelligence authorities in the [U. S.] with the fundamental rights of EU citizens whose data are transferred from the [EU] to the [U. S.], conflicts with the case made by the DPC to this court“.

73 – Viz čl. 1 odst. 1 a 3, jakož i body 14 až 16 odůvodnění rozhodnutí o štítu na ochranu soukromí.

74 – Probíhající věc T-738/16, La Quadrature du Net a další v. Komise (Úř. věst. 2017, C 6, s. 39).

180. Navíc, pokud by se Soudní dvůr vyslovil k výše popsaným problémům, narušil by podle mého názoru běžný průběh řízení, které má proběhnout poté, co vydá rozsudek v projednávané věci. V rámci uvedeného řízení musí DPC projednat stížnost M. Schremse s přihlédnutím k odpovědi, kterou Soudní dvůr poskytne na jedenáctou předběžnou otázku. Pokud Soudní dvůr rozhodne, jak navrhuji a v rozporu s tím, co před ním tvrdil DPC, že rozhodnutí 2010/87 není neplatné s ohledem na články 7, 8 a 47 Listiny, musí mít DPC podle mého názoru možnost přezkoumat spis týkající se řízení, které před ním probíhá. V případě, že bude mít DPC za to, že není schopen rozhodnout o stížnosti M. Schremse, aniž Soudní dvůr předtím určil, zda rozhodnutí o štítu na ochranu soukromí brání výkonu jeho pravomocí pozastavit dotčené předávání, a potvrdí, že má pochybnosti o platnosti tohoto rozhodnutí, bude moci se znovu obrátit na vnitrostátní soudy, aby se obrátily v tomto ohledu na Soudní dvůr⁷⁵.

181. Bylo by tedy zahájeno řízení, které by umožňovalo každému účastníku řízení a každé zúčastněné osobě uvedené v článku 23 druhém pododstavci jednacího řádu Soudního dvora předložit Soudnímu dvoru vyjádření týkající se konkrétně platnosti rozhodnutí o štítu na ochranu soukromí, a případně uvést konkrétní posouzení, která zpochybňuje, jakož i důvody, pro které má za to, že v něm Komise překročila omezený prostor pro volné uvážení, kterým disponovala⁷⁶. V rámci takového řízení by měla Komise příležitost přesně a podrobně odpovědět na každou z případných výtek proti uvedenému rozhodnutí. I když projednávaná věc poskytla účastníkům řízení a zúčastněným osobám, které předložily Soudnímu dvoru vyjádření, příležitost diskutovat o některých relevantních aspektech pro účely hodnocení souladu rozhodnutí o štítu na ochranu soukromí s články 7, 8 a 47 Listiny, tato otázka s ohledem na svůj význam zasluhuje, aby jí byla věnována vyčerpávající a důkladná diskuse.

182. Podle mého názoru obezřetnost vyžaduje vyčkat, až budou podniknuty tyto procesní kroky, předtím, než Soudní dvůr přezkoumá dopad, který má rozhodnutí o štítu na ochranu soukromí na to, jak orgán dozoru vyřídí návrh na pozastavení předávání prováděného do Spojených států podle čl. 46 odst. 1 GDPR, a rozhodne o platnosti tohoto rozhodnutí.

183. To platí tím spíše, že spis předložený Soudnímu dvoru neumožňuje dospět k závěru, že vyřízení stížnosti M. Schremse ze strany DPC bude nutně záviset na tom, zda rozhodnutí o štítu na ochranu soukromí brání tomu, aby orgány dozoru vykonaly svou pravomoc pozastavit předávání založené na standardních smluvních doložkách.

184. V tomto ohledu zaprvé není vyloučeno, že DPC pozastaví dotčené předávání z jiných důvodů, než jsou důvody týkající se údajné neodpovídající úrovně ochrany zajišťované ve Spojených státech proti zásahům do základních práv subjektů údajů, vyplývajícím z činností amerických zpravodajských služeb. Předkládající soud konkrétně upřesnil, že M. Schrems ve své stížnosti podané k DPC tvrdí, že smluvní doložky, kterých se společnost Facebook Ireland dovolává na podporu tohoto předávání, neodrážejí věrně doložky uvedené v příloze rozhodnutí 2010/87. M. Schrems mimoto tvrdí, že uvedené předávání spadá do působnosti nikoli tohoto rozhodnutí, ale ostatních rozhodnutí SSD⁷⁷.

185. Zadruhé DPC a předkládající soud zdůraznily, že společnost Facebook Ireland se na podporu předávání uvedeného ve stížnosti M. Schremse nedovolávala rozhodnutí o štítu na ochranu soukromí⁷⁸, což tato společnost na jednání potvrdila. I když společnost Facebook Inc. autocertifikovala (sama osvědčila) přijetí zásad štítu na ochranu soukromí od 30. září 2016⁷⁹, tvrdí, že toto přijetí se týká pouze předávání určitých kategorií údajů, a sice těch údajů, které se týkají obchodních partnerů

75 – Ostatně podotýkám, že v písemných vyjádřeních DPC nezaujal stanovisko k dopadu rozhodnutí o štítu na ochranu soukromí na vyřízení stížnosti, která je mu předložena.

76 – V tomto ohledu viz rozsudek Schrems (bod 78).

77 – Na podporu tohoto tvrzení M. Schrems tvrdí, že společnost Facebook Inc. musí být považována nejen za zpracovatele, ale rovněž za „správce“ ve smyslu čl. 4 bodu 7 GDPR, pokud jde o zpracovávání osobních údajů uživatelů sociální sítě Facebook. V tomto ohledu viz rozsudek ze dne 5. června 2018, Wirtschaftsakademie Schleswig-Holstein (C-210/16, EU:C:2018:388, bod 30).

78 – Viz rozsudek High Court (Vrchní soud) ze dne 3. října 2017 (bod 66).

79 – Viz internetové stránky „štítu na ochranu soukromí“ (https://www.privacyshield.gov/participant_search).

společnosti Facebook Inc. Považuji za nevhodné, aby Soudní dvůr předjímal otázky, které by v tomto ohledu mohly vyvstat, tím, že přezkoumá, zda by za předpokladu, že by se společnost Facebook Ireland nemohla dovolávat rozhodnutí 2010/87 na podporu dotčeného předávání, toto předávání nicméně spadalo do působnosti rozhodnutí o štítu na ochranu soukromí, i když posledně uvedená tento argument nevznesla před předkládajícím soudem ani před DPC.

186. Na základě toho mám za to, že není třeba odpovídat na druhou až pátou, jakož i devátou a desátou předběžnou otázku ani zkoumat platnost rozhodnutí o štítu na ochranu soukromí.

G. Podpůrné poznámky týkající se účinků a platnosti rozhodnutí o štítu na ochranu soukromí

187. Ačkoli mě výše uvedená analýza vede k tomu, že Soudnímu dvoru primárně navrhuji, aby se zdržel rozhodování o dopadu rozhodnutí o štítu na ochranu soukromí na vyřízení takové stížnosti, jako je stížnost podaná M. Schremsem u DPC, a o platnosti tohoto rozhodnutí, považuji za užitečné podpůrně a s výhradami uvést několik demonstrativních poznámek k této otázce.

1. K dopadu rozhodnutí o štítu na ochranu soukromí v rámci vyřízení stížnosti týkající se legality předávání na základě smluvních záruk orgánem dozoru

188. Devátá předběžná otázka nastoluje otázku, zda zjištění učiněné v rozhodnutí o štítu na ochranu soukromí týkající se odpovídající úrovně ochrany zajištěné ve Spojených státech s přihlédnutím k omezením přístupu k předávaným údajům a jejich využívání americkými orgány pro účely bezpečnosti státu, jakož i k právní ochraně subjektu údajů, brání tomu, aby orgán dozoru pozastavil předávání do této třetí země prováděné na základě standardních smluvních doložek.

189. Domnívám se, že tato problematika musí být posuzována s ohledem na body 51 a 52 rozsudku Schrems, ze kterých vyplývá, že vůči orgánům dozoru je rozhodnutí o odpovídající úrovni ochrany závazné, pokud není prohlášeno za neplatné. Orgán dozoru, ke kterému byla podána stížnost subjektu, jehož údaje jsou předávány do třetí země, na kterou se vztahuje rozhodnutí o odpovídající úrovni ochrany, tedy nemůže pozastavit předávání z důvodu neodpovídající úrovně ochrany, aniž Soudní dvůr předtím prohlásil toto rozhodnutí za neplatné⁸⁰.

190. Předkládající soud si v podstatě přeje zjistit, zda ohledně rozhodnutí o odpovídající úrovni ochrany – jako je rozhodnutí o štítu na ochranu soukromí nebo ještě před ním rozhodnutí o „bezpečném přístavu“ – které spočívá na dobrovolném přijetí zásad, které uvádí, podniky, tento závěr platí pouze tehdy, pokud se na předávání do dotčené třetí země vztahuje toto rozhodnutí, nebo rovněž tehdy, pokud předávání spočívá na odlišném právním základě.

191. Podle M. Schremse, německé, nizozemské, polské a portugalské vlády, jakož i Komise zjištění o odpovídající úrovni ochrany učiněné v rozhodnutí o štítu na ochranu soukromí nezbavuje orgány dozoru jejich pravomoci pozastavit nebo zakázat předávání do Spojených států prováděné na základě standardních smluvních doložek. Pokud se předávání do Spojených států neopírá o rozhodnutí o štítu na ochranu soukromí, nejsou orgány dozoru formálně vázány tímto rozhodnutím v rámci výkonu pravomocí, které jim přiznává čl. 58 odst. 2 GDPR. Jinými slovy, tyto orgány se mohou distancovat od zjištění Komise týkajících se odpovídající úrovně ochrany před zásahy amerických veřejných orgánů při výkonu základních práv subjektů údajů. Nizozemská vláda a Komise upřesňují, že orgány dozoru k tomu musí nicméně přihlédnout, když tyto pravomoci využívají. Podle názoru německé vlády mohou tyto orgány provést opačná posouzení až po meritorním přezkoumání zjištění provedených Komisí zahrnujícím relevantní šetření.

⁸⁰ – V tomto smyslu viz rozsudek Schrems (bod 59).

192. Naproti tomu společnost Facebook Ireland a vláda Spojených států v podstatě tvrdí, že závazný účinek rozhodnutí o odpovídající úrovni ochrany s ohledem na požadavky právní jistoty a jednotného použití unijního práva znamená, že orgány dozoru nejsou oprávněny zpochybnit zjištění obsažená v uvedeném rozhodnutí, a to ani v rámci vyřizování stížnosti směřující k pozastavení předávání do dotčené třetí země na jiném základě, než je toto rozhodnutí.

193. Souhlasím s prvním z těchto přístupů. Vzhledem k tomu, že působnost rozhodnutí o štítu na ochranu soukromí je omezena na předávání podniku, který se autocertifikoval (sám osvědčil) na základě tohoto rozhodnutí, uvedené rozhodnutí nemůže formálně zavazovat orgány dozoru, pokud jde o předávání, které do této působnosti nespadá. Rozhodnutí o štítu na ochranu soukromí má za účel zajištění právní jistoty pouze ve prospěch vývozců, kteří předávají údaje v rámci, který zavádí. Podle mého názoru nezávislost, kterou článek 52 GDPR přiznává orgánům dozoru, směřuje rovněž k zabránění tomu, aby tyto orgány byly vázány zjištěními vyhotovenými Komisí v rozhodnutí o odpovídající úrovni ochrany nad rámec jeho působnosti.

194. Samozřejmě zjištění uvedená v rozhodnutí o štítu na ochranu soukromí týkající se odpovídající úrovně ochrany zajištěné ve Spojených státech před zásahy spojenými s činnostmi jejich zpravodajských služeb, představují výchozí bod analýzy, kterou orgán dozoru případ od případu posuzuje, zda předávání založené na standardních smluvních doložkách musí být pozastaveno z důvodu takových zásahů. Má-li však po důkladném šetření za to, že se nebude moci připojit k těmto zjištěním ohledně předávání, na které byl upozorněn, příslušný orgán dozoru si podle mého názoru zachovává možnost vykonávat své pravomoci, které mu přiznává čl. 58 odst. 2 písm. f) a j) GDPR.

195. Za předpokladu, že by však Soudní dvůr odpověděl na zde zkoumanou otázku opačně, než jak navrhuji, bylo by třeba zkoumat, zda by tyto pravomoci neměly přesto být obnoveny z důvodu neplatnosti rozhodnutí o štítu na ochranu soukromí.

2. K platnosti rozhodnutí o štítu na ochranu soukromí

196. Následující poznámky vyvolávají určité otázky týkající se opodstatněnosti posouzení uvedených v rozhodnutí o štítu na ochranu soukromí ohledně odpovídající úrovně ochrany zajištěné Spojenými státy ve smyslu čl. 45 odst. 1 GDPR z hlediska činností dozoru nad elektronickými komunikacemi prováděnými americkými zpravodajskými orgány. Tyto poznámky nemají za cíl vyjádřit konečné nebo vyčerpávající stanovisko ohledně platnosti tohoto rozhodnutí. Omezují se na poskytnutí určitých úvah, které by se mohly ukázat jako užitečné pro Soudní dvůr v případě, že by na rozdíl od toho, co navrhuji, hodlal o této otázce rozhodnout.

197. V tomto ohledu z bodu 64 odůvodnění a bodu I.5 přílohy II rozhodnutí o štítu na ochranu soukromí vyplývá, že přijetí v tomto rozhodnutí uvedených zásad podniky může být omezeno zejména požadavky týkajícími se národní bezpečnosti, veřejného zájmu a dodržování právních předpisů nebo protichůdnými povinnostmi vyplývajícími z amerického práva.

198. Komise proto posoudila záruky stanovené v právu Spojených států ohledně přístupu k předávaným údajům a jejich využívání americkými veřejnými orgány pro účely zejména národní bezpečnosti⁸¹. Od americké vlády obdržela určité závazky týkající na straně jedné omezení přístupu k předávaným údajům a jejich využívání americkými orgány, jakož i na straně druhé právní ochrany subjektů údajů⁸².

81 – Viz bod 65 odůvodnění rozhodnutí o štítu na ochranu soukromí.

82 – Viz přílohy III až VII rozhodnutí o štítu na ochranu soukromí.

199. V řízení před Soudním dvorem se M. Schrems dovolává neplatnosti rozhodnutí o štítu na ochranu soukromí z důvodu, že takto popsané záruky nepostačují k zajištění odpovídající úrovně ochrany základních práv subjektů, jejichž údaje jsou předávány do Spojených států. DPC, EPIC, jakož i rakouská, polská a portugalská vláda zpochybňují posouzení, která v něm provedla Komise ohledně odpovídající úrovně ochrany před zásahy plynoucími z činností amerických zpravodajských služeb, aniž přímo zpochybňují platnost tohoto rozhodnutí. Tyto pochybnosti vycházejí z obav vyjádřených Parlamentem⁸³, EDPB⁸⁴ a EIOÚ⁸⁵.

200. Před přezkumem opodstatněnosti zjištění o odpovídající úrovni ochrany provedeného v rozhodnutí o štítu na ochranu soukromí je nezbytné upřesnit metodiku, kterou se má tento přezkum řídit.

a) Upřesnění týkající se obsahu přezkumu platnosti rozhodnutí o odpovídající úrovni ochrany

1) K obsahu srovnání, které umožňuje posoudit „podstatnou rovnocennost“ úrovně ochrany

201. V souladu s čl. 45 odst. 3 GDPR a judikaturou Soudního dvora⁸⁶ může Komise konstatovat, že určitá třetí země zajišťuje odpovídající úroveň ochrany, pouze pokud dospěla k řádně odůvodněnému závěru, že úroveň ochrany základních práv subjektů údajů je v této zemi „v zásadě rovnocenná“ úrovni, která je vyžadována v Unii na základě tohoto nařízení vykládaného ve světle Listiny.

202. Ověření odpovídající úrovně ochrany zajištěné ve třetí zemi tak nutně vyžaduje srovnání pravidel a zvyklostí v této třetí zemi na jedné straně s pravidly ochrany platnými v Unii na straně druhé. Ve své druhé otázce žádá předkládající soud Soudní dvůr, aby upřesnil obsah tohoto srovnání⁸⁷.

203. Konkrétně se daný soud snaží zjistit, zda výhrada pravomoci, kterou čl. 4 odst. 2 SEU a čl. 2 odst. 2 GDPR přiznávají členským státům v oblasti ochrany národní bezpečnosti, znamená, že unijní právní řád neobsahuje standardy ochrany, se kterými by měly být za účelem posouzení své odpovídající povahy srovnávány záruky ve třetí zemi pro zpracovávání údajů, které jsou do této země předávány, veřejnými orgány pro účely ochrany národní bezpečnosti. Pro případ kladné odpovědi pokládá uvedený soud dotaz, jak musí být určen relevantní referenční rámec.

83 – Usnesení Evropského parlamentu ze dne 6. dubna 2017 o přiměřenosti ochrany poskytované štítem EU–USA na ochranu soukromí, P8_TA(2017)0131, a ze dne 5. července 2018 o přiměřenosti ochrany poskytované štítem EU–USA na ochranu soukromí, P8_TA(2018)0315.

84 – Viz pracovní skupina pro ochranu osobních údajů zřízená podle článku 29 (dál jen „Skupina 29“), Opinion 1/2016 on the EU–U. S. Privacy Shield draft adequacy decision, 13. dubna 2016, WP 238; Skupina 29, EU-US Privacy Shield – First Annual Joint Review, 28. listopadu 2017, WP 255, a EDPB, EU-US Privacy Shield – Second Annual Joint Review, 22. ledna 2019. Skupina 29 byla založena na základě čl. 29 odst. 1 směrnice 95/46, který stanovil její poradní a nezávislou povahu. Podle odstavce 2 tohoto článku v této skupině bylo po zástupci každého z orgánů dozoru určených jednotlivými členskými státy, po zástupci každého z orgánů vytvořených pro orgány a instituce Společenství, jakož i zástupce Komise. Od vstupu GDPR v platnost byla Skupina 29 nahrazena EDPB (viz čl. 94 odst. 2 tohoto nařízení).

85 – Viz EIOÚ, stanovisko 4/2016, týkající se „štítu na ochranu soukromí EU–USA“ (Privacy Shield) – Návrh rozhodnutí o odpovídající úrovni ochrany ze dne 30. května 2016. EIOÚ byl zřízen čl. 1 odst. 2 nařízení Evropského parlamentu a Rady (ES) č. 45/2001 ze dne 18. prosince 2000 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány a institucemi Společenství a o volném pohybu těchto údajů (Úř. věst. 2001, L 8, s. 1; Zvl. vyd. 13/26, s. 102). Dohlíží na dodržování ustanovení tohoto nařízení.

86 – Viz bod 112 tohoto stanoviska.

87 – Připomínám, že podstatná rovnocennost úrovně ochrany zaručené třetím státem ve vztahu k úrovni, která je vyžadována v Unii, musí být rovněž posouzena, pokud v rámci konkrétního předávání založeného na standardních smluvních doložkách stanovených v rozhodnutí 2010/87 správce, nebo v případě, že to není možné, příslušný orgán dozoru ověří, zda veřejné orgány třetí země určení ukládají dovozci požadavky, které překračují meze toho, co je nezbytné v demokratické společnosti (viz doložka 5 obsažená v příloze rozhodnutí 2010/87, jakož i související poznámka pod čarou). Viz body 115, 134 a 135 tohoto stanoviska.

204. V tomto ohledu je třeba mít na paměti, že důvodem existence omezení, která unijní právo stanoví z hlediska mezinárodního předávání osobních údajů tím, že vyžaduje, aby byla zajištěna kontinuita úrovně ochrany práv subjektů údajů, je zabránit riziku obcházení standardů použitelných v rámci Unie⁸⁸. Jak v podstatě tvrdí společnost Facebook Ireland, vzhledem k tomuto cíli není nijak odůvodněné počítat s tím, že třetí země bude splňovat požadavky, které neodpovídají povinnostem, které jsou uloženy členským státům.

205. V souladu s čl. 51 odst. 1 Listiny je přitom Listina určena členským státům, výhradně pokud uplatňují unijní právo. V důsledku toho platnost rozhodnutí o odpovídající úrovni ochrany s ohledem na omezení výkonu základních práv subjektů údajů, která vyplývají z právní úpravy třetí země určení, závisí na srovnání těchto omezení s omezeními, která by ze strany členských států umožňovala ustanovení Listiny, *pouze v rozsahu, v němž by podobná právní úprava členského státu spadala do působnosti unijního práva*.

206. Odpovídající úroveň ochrany zajištěná ve třetím státě určení však nemůže být posuzována bez ohledu na případné zásahy do výkonu základních práv subjektů údajů, které by vyplývaly ze státních opatření, zejména v oblasti národní bezpečnosti, která, pokud by byla přijata členským státem, by nespadala do působnosti unijního práva. Pro účely tohoto posouzení čl. 45 odst. 2 písm. a) GDPR vyžaduje bez jakéhokoli omezení zohlednit právní předpisy v oblasti národní bezpečnosti.

207. Posouzení odpovídající úrovně ochrany s ohledem na taková státní opatření podle mého názoru znamená, že je třeba porovnat záruky, které jsou s ní spojeny, s úrovní ochrany vyžadované v rámci Unie podle právních předpisů členských států, včetně jejich závazků vyplývajících z EÚLP. Vzhledem k tomu, že přistoupení členských států k EÚLP ukládá těmto členským státům povinnost zajistit soulad jejich vnitrostátního práva s ustanoveními této úmluvy, a představuje tak, jak v podstatě zdůraznily společnost Facebook Ireland, německá a česká vláda, jakož i Komise, společný jmenovatel pro členské státy, budu považovat tato ustanovení za relevantní srovnávací kritérium pro účely tohoto posouzení.

208. Jak bylo uvedeno výše⁸⁹, v projednávaném případě mají požadavky týkající se národní bezpečnosti Spojených států přednost před povinnostmi autocertifikovaných podniků na základě rozhodnutí o štítu na ochranu soukromí. Rovněž platnost tohoto rozhodnutí závisí na tom, zda jsou s těmito požadavky spojeny záruky, které poskytují v zásadě rovnocennou úroveň ochrany s úrovní ochrany, která musí být zajištěna v Unii.

209. Odpověď na tuto otázku vyžaduje určit předem standardy – a sice standardy vycházející z Listiny nebo EÚLP – které by měly v rámci Unie splňovat právní předpisy v oblasti dozoru nad elektronickými komunikacemi, které jsou podobné těm, které Komise přezkoumala v rozhodnutí o štítu na ochranu soukromí. Určení použitelných standardů závisí na tom, zda by se na takové právní předpisy, jako je článek 702 FISA a EO 12333, vztahovalo, pocházely-li by z členského státu, omezení působnosti GDPR na základě čl. 2 odst. 2 tohoto nařízení vykládaného ve světle čl. 4 odst. 2 SEU.

210. V této souvislosti ze znění čl. 4 odst. 2 SEU a ustálené judikatury vyplývá, že unijní právo, a zejména nástroje sekundárního práva týkající se ochrany osobních údajů, se nevztahuje na činnosti v oblasti ochrany národní bezpečnosti v rozsahu, v němž představují činnosti, jež jsou vlastní státům nebo státním orgánům a nemají nic společného s činnostmi jednotlivců⁹⁰.

⁸⁸ – Viz bod 117 tohoto stanoviska.

⁸⁹ – Viz bod 197 tohoto stanoviska.

⁹⁰ – Viz zejména rozsudky ze dne 6. listopadu 2003, Lindqvist (C-101/01, EU:C:2003:596, body 43 a 44); PNR (bod 58); ze dne 16. prosince 2008, Satakunnan Markkinapörssi a Satamedia (C-73/07, EU:C:2008:727, bod 41); ze dne 21. prosince 2016, Tele2 Sverige a Watson a další (C-203/15 a C-698/15, EU:C:2016:970, dále jen „rozsudek Tele2 Sverige“, bod 69), jakož i ze dne 2. října 2018, Ministerio Fiscal (C-207/16, EU:C:2018:788, dále jen „rozsudek Ministerio Fiscal“, bod 32).

211. Tato zásada *zaprvné* znamená, že právní úprava v oblasti ochrany národní bezpečnosti nespadá do působnosti unijního práva, pokud upravuje výlučně státní činnosti, a tedy neupravuje jakoukoli činnost vykonávanou jednotlivci. Podle mého názoru se toto právo nepoužije na vnitrostátní opatření týkající se shromažďování a využívání osobních údajů, která stát přímo provádí za účelem ochrany národní bezpečnosti, aniž ukládá konkrétní povinnosti soukromým subjektům. Jak zejména tvrdila Komise na jednání, opatření přijaté členským státem, které podobně jako EO 12333 umožňuje přímý přístup jeho bezpečnostních služeb k předávaným údajům, je vyloučeno z působnosti unijního práva⁹¹.

212. Podstatně složitější je otázka, zda *zadruhé* vnitrostátní ustanovení, která stejným způsobem jako článek 702 FISA ukládají poskytovatelům služeb elektronických komunikací, aby poskytovali podporu příslušným orgánům v oblasti národní bezpečnosti, a umožnili jim tak přístup k určitým osobním údajům, spadají rovněž mimo působnost unijního práva.

213. Zatímco rozsudek PNR hovoří ve prospěch kladné odpovědi na tuto otázku, úvahy uvedené v rozsudcích Tele2 Sverige a Ministerio Fiscal mohou odůvodňovat, aby na ni bylo odpovězeno záporně.

214. V rozsudku PNR Soudní dvůr zrušil rozhodnutí, v němž Komise konstatovala odpovídající úroveň ochrany osobních údajů obsažených v záznamech o knihování cestujících v letecké dopravě (Passenger Name Records, PNR) předávaných příslušnému americkému orgánu pro cla a ochranu hranic⁹². Soudní dvůr rozhodl, že zpracování, jehož se týkalo toto rozhodnutí – a sice předávání údajů PNR leteckými společnostmi dotčenému orgánu – spadalo *s ohledem na svůj předmět* do vyloučení z působnosti směrnice 95/46 stanovené v čl. 3 odst. 2. Podle Soudního dvora bylo toto zpracování nezbytné nikoliv pro poskytnutí služeb, ale pro ochranu veřejné bezpečnosti a k trestním účelům. Vzhledem k tomu, že dotčené předávání spadalo do rámce zřízeného orgány veřejné moci a týkajícího se veřejné bezpečnosti, bylo vyloučeno z působnosti této směrnice navzdory skutečnosti, že údaje PNR byly původně shromažďovány soukromými subjekty v rámci obchodní činnosti spadající do této působnosti a toto předávání bylo těmito subjekty organizováno⁹³.

215. V následujícím rozsudku Tele2 Sverige⁹⁴ Soudní dvůr rozhodl, že vnitrostátní předpisy založené na čl. 15 odst. 1 směrnice 2002/58/ES⁹⁵, které upravují uchovávání provozních a lokalizačních údajů poskytovateli telekomunikačních služeb i přístup ze strany veřejných orgánů k uchovávaným údajům pro účely uvedené v tomto ustanovení – které zahrnují trestní stíhání a ochranu národní bezpečnosti – tudíž spadají do působnosti této směrnice, a tedy i Listiny. Podle Soudního dvora se na ustanovení

91 – Aby v tomto bodě nedošlo k nepochopení, zdůrazňuji, že v rozhodnutí o štítu na ochranu soukromí nebyla Komise schopna určit, zda Spojené státy skutečně zadržovaly sdělení přenášená prostřednictvím transatlantických kabelů, jelikož americké orgány tento návrh nepotvrdily ani nevyvrátily [viz bod 75 odůvodnění tohoto rozhodnutí, jakož i dopis Roberta Litta ze dne 22. února 2016, který je obsažen v jeho příloze VI bodě I písm. a)]. Nicméně vzhledem k tomu, že vláda Spojených států nepopřela, že shromažďuje předávané údaje na základě EO 12333, musela Komise podle mého názoru dosáhnout před tím, než provede zjištění o odpovídající úrovni ochrany, získat od této vlády ujištění, podle kterých takové shromažďování, v případě, že by k němu došlo, bylo spojeno s dostatečnými zárukami proti riziku zneužití. V této souvislosti Komise v bodech 68 až 77 odůvodnění uvedeného rozhodnutí přezkoumala omezení a záruky, které by se měly použít v takovém případě na základě PPD 28.

92 – Jednalo se o rozhodnutí Komise 2004/535/ES ze dne 14. května 2004 o odpovídající úrovni ochrany osobních údajů obsažených v záznamech o knihování cestujících v letecké dopravě, které se předávají Úřadu USA pro cla a ochranu hranic (Úř. věst. 2004, L 235, s. 11).

93 – Rozsudek PNR (body 56 až 58). Kromě toho v rozsudku ze dne 10. února 2009, Irsko v. Parlament a Rada (C-301/06, EU:C:2009:68, body 90 a 91), Soudní dvůr rozhodl, že úvahy rozvinuté v rozsudku PNR nelze použít ve vztahu ke zpracování uvedenému ve směrnici Evropského parlamentu a Rady 2006/24/ES ze dne 15. března 2006 o uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí a o změně směrnice 2002/58/ES (Úř. věst. 2006, L 105, s. 54). Soudní dvůr odůvodnil tento závěr skutečností, že na rozdíl od rozhodnutí dotčeného v rozsudku PNR se směrnicí 2006/24 týkala pouze činnosti poskytovatelů služeb na vnitřním trhu a neobsahuje žádnou právní úpravu činnosti orgánů veřejné moci za trestněprávními účely. Zdá se, že na základě těchto úvah Soudní dvůr potvrdil, že závěr vycházející z rozsudku PNR je *a contrario* použitelný na ustanovení týkající se přístupu k uchovávaným údajům nebo jejich využívání těmito orgány.

94 – Rozsudek Tele2 Sverige (body 67 až 81).

95 – Směrnice Evropského parlamentu a Rady ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (Směrnice o soukromí a elektronických komunikacích) (Úř. věst. 2002, L 201, s. 37; Zvl. vyd. 13/29, s. 514).

týkající se uchovávání údajů, ani na ustanovení týkající se přístupu k uchovávaným údajům nevztahuje vyloučení z působnosti této směrnice stanovené v jejím čl. 1 odst. 3, který odkazuje zejména na činnosti státu v oblasti trestního stíhání a ochrany národní bezpečnosti⁹⁶. Soudní dvůr tuto judikaturu potvrdil v rozsudku *Ministerio Fiscal*⁹⁷.

216. Článek 702 FISA se však od takové právní úpravy liší tím, že toto ustanovení neukládá poskytovatelům služeb elektronických komunikací povinnost uchovávat údaje, ani povinnost provádět jakékoli zpracování v případě neexistence žádosti o přístup k údajům od zpravodajských orgánů.

217. Vystává tedy otázka, zda do působnosti GDPR, a tudíž do působnosti Listiny, spadají vnitrostátní opatření, která těmto poskytovatelům ukládají povinnost zpřístupnit údaje veřejným orgánům pro účely národní bezpečnosti *nezávisle na jakékoli povinnosti uchovávat údaje*⁹⁸.

218. *První přístup* může spočívat v uvedení, pokud je to možné, obou výše uvedených linií judikatury do souladu na základě výkladu závěru Soudního dvora v rozsudcích *Tele2 Sverige* a *Ministerio Fiscal*, který se týká použitelnosti unijního práva na opatření, která upravují přístup k údajům vnitrostátními orgány za účelem zejména ochrany národní bezpečnosti⁹⁹, tak, že by se omezovalo na případy, ve kterých byly údaje uchovávány *na základě zákonné povinnosti* zavedené na základě čl. 15 odst. 1 směrnice 2002/58. Tento závěr se naproti tomu nepoužije na skutkový kontext odlišný od rozsudku PNR, který se týkal předávání údajů uchovávaných leteckými společnostmi za obchodním účelem z jejich vlastního podnětu americkému orgánu příslušnému v oblasti vnitřní bezpečnosti.

219. Podle *druhého přístupu*, který Komise prosazuje a který považuji za přesvědčivější, odůvodňují úvahy uvedené v rozsudcích *Tele2 Sverige* a *Ministerio Fiscal* použitelnost unijního práva na vnitrostátní pravidla ukládající poskytovatelům služeb elektronických komunikací povinnost poskytnout pomoc orgánům příslušným v oblasti národní bezpečnosti k tomu, aby mohly získat přístup k určitým údajům, *aniž je nutné, aby tato pravidla stanovila povinnost předchozího uchovávání údajů*.

220. Jádrem této úvahy totiž není předmět dotčených ustanovení jako v rozsudku PNR, nýbrž skutečnost, že tato ustanovení upravovala činnosti poskytovatelů tím, že jim ukládala zpracování údajů. Tyto činnosti nepředstavovaly činnosti státu v oblastech uvedených v čl. 1 odst. 3 směrnice 2002/58 a v čl. 3 odst. 2 směrnice 95/46, jejichž obsah v podstatě přebírá čl. 2 odst. 2 GDPR.

96 – Vzhledem k tomu, že směrnice 2002/58 konkretizuje požadavky směrnice 95/46, kterou zrušilo GDPR, jež do značné míry přebírá její obsah, je podle mého názoru judikatura týkající se výkladu čl. 1 odst. 3 směrnice 2002/58 použitelná *per analogiam* i na výklad čl. 2 odst. 2 GDPR. V tomto smyslu viz rozsudky *Tele2 Sverige* (bod 69) a *Ministerio Fiscal* (bod 32).

97 – Rozsudek *Ministerio Fiscal* (body 34, 35 a 37).

98 – Tatáž otázka byla vznesena v rámci tří jiných řízení o předběžné otázce probíhajících před Soudním dvorem. Viz věc C-623/17, *Privacy International* (Úř. věst. 2018, C 22, s. 29), jakož i spojené věci C-511/18 a C-512/18, *La Quadrature du Net* a další a *French Data Network* a další (Úř. věst. 2018, C 392, s. 7).

99 – I když se Soudní dvůr v rozsudku *Tele2 Sverige* soustředil na přezkum odůvodnění zásahů vyplývajících z dotčeného uchovávání a přístupu s ohledem na cíl boje proti trestné činnosti, závěr, ke kterému dospěl, platí *mutatis mutandis* rovněž tehdy, pokud taková opatření sledují cíl ochrany národní bezpečnosti. Článek 15 odst. 1 směrnice 2002/58 totiž mezi cíli, které mohou odůvodňovat taková opatření, uvádí boj proti trestné činnosti i ochranu národní bezpečnosti. Kromě toho čl. 1 odst. 3 směrnice 2002/58 a čl. 2 odst. 2 GDPR vylučují z působnosti těchto předpisů činnosti státu v oblasti národní bezpečnosti i v trestní oblasti. Opatření dotčená ve věci, ve které byl vydán rozsudek *Tele2 Sverige*, ostatně sledovala rovněž cíl spojený s národní bezpečností. V bodě 119 uvedeného rozsudku se Soudní dvůr výslovně zabýval odůvodněním opatření týkajících se uchovávání provozních a lokalizačních údajů a přístupu k nim s ohledem na cíl ochrany národní bezpečnosti v rozsahu, v němž zahrnuje boj proti terorismu.

221. V rozsudku Tele2 Sverige tak Soudní dvůr uvedl, že „přístup k údajům uchovávaným [...] poskytovateli[se] týká zpracování osobních údajů ze strany uvedených poskytovatelů, na které se vztahuje oblast působnosti této směrnice“¹⁰⁰. Stejně tak rozhodl v rozsudku Ministerio Fiscal, že legislativní opatření ukládající poskytovatelům povinnost zpřístupnit uchovávané údaje příslušným orgánům „nutně znamená, že *tito poskytovatelé* s [těmito] údaji nakládají [tyto údaje zpracovávají]“¹⁰¹.

222. Zpřístupnění údajů správcem ve prospěch veřejného orgánu přitom odpovídá definici „zpracování“ uvedené v čl. 4 bodě 2 GDPR¹⁰². Totéž platí pro předchozí filtraci údajů prostřednictvím vyhledávacích kritérií pro účely izolace těch, ke kterým veřejné orgány požadovaly přístup¹⁰³.

223. Z toho vyvozují, že podle úvah Soudního dvora v rozsudcích Tele2 Sverige a Ministerio Fiscal se GDPR, a tudíž i Listina, použijí na vnitrostátní právní úpravu, která ukládá poskytovateli služeb elektronických komunikací, aby poskytoval pomoc orgánům příslušným v oblasti národní bezpečnosti tím, že jim poskytne údaje, případně i poté, co je profiltruje, i nezávisle na jakékoli zákonné povinnosti uchovávat těchto údajů.

224. Tento výklad navíc vyplývá přinejmenším implicitně z rozsudku Schrems. Jak zdůraznili DPC, rakouská a polská vláda, jakož i Komise, Soudní dvůr v rámci přezkumu platnosti rozhodnutí o „bezpečném přístavu“ v daném rozsudku rozhodl, že právo třetí země, na kterou se vztahuje rozhodnutí o odpovídající úrovni ochrany, musí stanovit záruky před zásahy svých veřejných orgánů do základních práv subjektů údajů pro účely národní bezpečnosti, které jsou v zásadě rovnocenné zárukám, které vyplývají zejména z článků 7, 8 a 47 Listiny¹⁰⁴.

225. Z toho konkrétně vyplývá, že vnitrostátní opatření, které poskytovatelům služeb elektronických komunikací ukládá, aby vyhověli žádosti příslušných orgánů v oblasti národní bezpečnosti státu o přístup k určitým údajům uchovávaným těmito poskytovateli v rámci jejich obchodních činností nezávisle na jakékoli zákonné povinnosti, tím, že předem určí údaje požadované použitím selektorů (stejně jako v rámci programu PRISM), nespadá do působnosti čl. 2 odst. 2 GDPR. Stejně je tomu v případě vnitrostátního opatření, které od podniků provozujících „páteří sítě“ telekomunikací vyžaduje, aby poskytly orgánům příslušným v oblasti národní bezpečnosti přístup k údajům, které procházejí přes infrastrukturu, kterou provozují (jako v rámci programu Upstream).

226. Naproti tomu jsou-li údaje, o něž se jedná, v rukou státních orgánů, jejich uchovávaní a jejich následné využití těmito orgány pro účely národní bezpečnosti je podle mého názoru ze stejných důvodů, jako jsou důvody uvedené v bodě 211 tohoto stanoviska, pokryto výjimkou stanovenou v čl. 2 odst. 2 GDPR, takže nespadá do působnosti tohoto nařízení, a tudíž ani do působnosti Listiny.

227. S ohledem na výše uvedené mám za to, že přezkum platnosti rozhodnutí o štítu na ochranu soukromí s ohledem na omezení zásad v něm uvedených, které mohou vyplývat z činností amerických zpravodajských orgánů, s sebou nese dvojí ověření.

100 – Rozsudek Tele2 Sverige (bod 78, kurzivou zvýraznil autor stanoviska stanoviska). Jak o tom svědčí použití výrazu „[d]ále“, Soudní dvůr v bodě 79 uvedeného rozsudku zdůraznil úzkou souvislost mezi povinností uchovávat dotčené údaje ve věci, ve které byl rozsudek vydán, a ustanoveními týkajícími se přístupu vnitrostátních orgánů k uchovávaným údajům pouze na podporu svého závěru týkajícího se použitelnosti směrnice 2002/58.

101 – Rozsudek Ministerio Fiscal (bod 37, kurzivou zvýraznil autor stanoviska stanoviska).

102 – V tomto smyslu viz rozsudek Ministerio Fiscal (bod 38).

103 – V tomto smyslu viz rozsudek ze dne 13. května 2014, Google Spain a Google (C-131/12, EU:C:2014:317, bod 28).

104 – Rozsudek Schrems (body 91 až 96). V bodech 90, 124 a 141 odůvodnění rozhodnutí o štítu na ochranu soukromí Komise ostatně odkazuje na ustanovení Listiny, čímž souhlasí se zásadou, podle které musí být omezení základních práv, která odpovídají cíli ochrany národní bezpečnosti, v souladu s Listinou.

228. *Zaprvé* bude třeba zkoumat, zda Spojené státy zajišťují úroveň ochrany, která je v zásadě rovnocenná úrovni ochrany vyplývající z ustanovení GDPR a Listiny, proti omezením vyplývajícím z použití článku 702 FISA v rozsahu, v němž toto ustanovení umožňuje NSA ukládat poskytovatelům povinnost zpřístupnit jí osobní údaje.

229. *Zadruhé* ustanovení EÚLP představují relevantní referenční rámec za účelem posouzení, zda omezení, která by mohlo způsobit provedení EO 12333 tím, že opravňuje zpravodajské orgány k tomu, aby samy bez pomoci soukromých subjektů shromažďovaly osobní údaje, zpochybňují odpovídající úroveň ochrany zajištěné ve Spojených státech. Tato ustanovení poskytují rovněž srovnávací standardy, které umožňují posoudit odpovídající povahu této úrovně ochrany z hlediska uchovávání a využití údajů získaných těmito orgány pro účely národní bezpečnosti.

230. Je však ještě třeba určit, zda zjištění odpovídající úrovně ochrany předpokládá, že shromažďování údajů na základě EO 12333 je spojeno s úrovní ochrany, která je v podstatě rovnocenná úrovni ochrany, která musí být zajištěna v rámci Unie, a *to v rozsahu, v němž se toto shromažďování uskutečňuje mimo území Spojených států*, během fáze předávání údajů z Unie do této třetí země.

2) K nezbytnosti zajistit odpovídající úroveň ochrany během předávání údajů

231. Před Soudním dvorem byly obhajovány tři odlišné postoje ohledně nezbytnosti toho, aby Komise pro účely posouzení odpovídající úrovně ochrany zajištěné ve třetí zemi zohlednila vnitrostátní opatření týkající se přístupu k údajům ze strany orgánů této třetí země mimo jeho území, během předávání údajů z Unie na toto území.

232. *Zaprvé* společnost Facebook Ireland, jakož i vláda Spojených států a Spojené království v podstatě tvrdí, že existence takových opatření nemá v rámci zjištění o odpovídající úrovni ochrany žádný dopad. Tito poslední uvedení se na podporu tohoto přístupu dovolávají toho, že třetí stát nemůže kontrolovat všechny komunikační prostředky nacházející se mimo jeho území, kterými se předávají údaje pocházející z Unie, takže nelze nikdy již z povahy věci zaručit, že v průběhu jejich předávání jiný stát údaje tajně neshromáždí.

233. *Zadruhé* DPC, M. Schrems, EPIC, rakouská a nizozemská vláda, Parlament a EDPB tvrdí, že požadavek kontinuity úrovně ochrany, uvedený v článku 44 GDPR, znamená, že tato úroveň musí být odpovídající po celou dobu předávání, a to i tehdy, jsou-li údaje předávány podmořskými kabely před dosažením území třetí země určení.

234. Ačkoli Komise tuto zásadu uznává, zatřetí tvrdí, že předmět zjištění o odpovídající úrovni ochrany se omezuje na ochranu zajišťovanou třetí zemí *v rámci jejích hranic*, takže okolnost, že v průběhu *předávání* do této třetí země není zajištěna odpovídající úroveň ochrany, nezpochybňuje platnost rozhodnutí o odpovídající úrovni ochrany. Je nicméně na správci, aby v souladu s článkem 32 GDPR zajistil bezpečnost předávání a co nejvíce ochránil osobní údaje při předávání do uvedené třetí země.

235. V tomto ohledu podotýkám, že článek 44 GDPR podmiňuje předání do třetí země splněním podmínek stanovených v ustanoveních kapitoly V tohoto nařízení, jelikož údaje mohou být „po předání“ zpracovány. Tento výraz by mohl být chápán tak, že znamená, jak tvrdila vláda Spojených států ve své písemné odpovědi na otázky Soudního dvora, že tyto podmínky musí být splněny *po předání údajů do místa určení*, nebo že je naopak nutné je plnit poté, co bylo předávání zahájeno (tedy včetně fáze předávání).

236. Vzhledem k tomu, že znění článku 44 GDPR není jednoznačné, vede mě teleologický výklad k přijetí druhého z těchto výkladů, a tudíž se připojuji k druhému z výše uvedených přístupů. Pokud by se totiž mělo za to, že požadavek kontinuity úrovně ochrany stanovený v tomto ustanovení zahrnuje pouze opatření dozoru prováděná na území třetí země určení, by bylo možné ho obcházet,

pokud tato třetí země uplatňuje taková opatření mimo své území ve fázi předávání údajů. Proto, aby se předešlo tomuto riziku, musí se posouzení odpovídající úrovně ochrany zajištěné třetí zemí vztahovat na všechna ustanovení právního řádu této třetí země, zejména v oblasti národní bezpečnosti¹⁰⁵, k nimž patří ustanovení týkající se dozoru prováděného nad jeho územím i ustanovení, která umožňují dozor nad údaji předávanými na toto území¹⁰⁶.

237. Nikdo však nezpochybňuje, jak zdůraznil EDPB, že se posouzení odpovídající úrovně ochrany týká výlučně ustanovení právního řádu *třetí země určené údajů*, jak vyplývá z čl. 45 odst. 1 GDPR. Nemožnost zaručit, že jiný třetí stát neshromažďuje tyto údaje v průběhu jejich předávání, již se dovolává společnost Facebook Ireland, jakož i vláda Spojených států a Spojeného království, toto posouzení neovlivňuje. Takové riziko nemůže být ostatně vyloučeno ani poté, co údaje dorazily na území třetího státu určené.

238. Kromě toho je rovněž skutečností, že Komisi při posuzování odpovídající úrovně ochrany zaručené třetí zemí může případně tato třetí země opomenout informovat o existenci určitých tajných sledovacích programů. Z toho však nevylučuje, že *pokud jsou jí takové programy oznámeny*, může Komise upustit od jejich zohlednění v rámci svého přezkumu odpovídající úrovně. Stejně tak pokud je Komisi po přijetí rozhodnutí o odpovídající úrovni ochrany sdělena existence určitých tajných programů sledování prováděných třetí zemí na jejím území nebo během předávání do této země, je povinna přezkoumat svá zjištění týkající se odpovídající úrovně ochrany zajištěné touto třetí zemí, pokud takové sdělení vyvolává v tomto ohledu pochybnosti¹⁰⁷.

3) K zohlednění skutkových zjištění provedených Komisí a předkládajícím soudem ohledně práva Spojených států

239. I když je nesporné, že Soudní dvůr není příslušný k výkladu práva třetí země, který by byl v právním řádu této země závazný, závisí platnost rozhodnutí o štítu na ochranu soukromí na opodstatněnosti posouzení provedeného Komisí ohledně úrovně ochrany zajištěné právem a zvyklostmi Spojených států z hlediska základních práv osob, jejichž údaje jsou předávány do této třetí země. Komise je totiž povinna odůvodnit své zjištění o odpovídající úrovni ochrany z hlediska skutečností uvedených v čl. 45 odst. 2 GDPR, které se týkají zejména obsahu práva uvedené třetí země¹⁰⁸.

240. High Court (Vrchní soud) ve svém rozsudku ze dne 3. října 2017 uvedl podrobná zjištění, která popisují relevantní aspekty amerického práva, poté, co posoudil důkazy předložené stranami sporu¹⁰⁹. Toto vyličení do značné míry překrývá zjištění Komise v rozhodnutí o štítu na ochranu soukromí vztahující se k obsahu pravidel týkajících se shromažďování a přístupu amerických zpravodajských orgánů k předávaným údajům, jakož i k prostředkům nápravy a mechanismům dozoru nad těmito činnostmi.

241. Předkládající soud, stejně jako několik účastníků a zúčastněných stran, kteří Soudnímu dvoru předložili vyjádření, zpochybňují spíše právní důsledky, které Komise vyvodila z těchto zjištění – a sice závěr, že Spojené státy zajišťují odpovídající úroveň ochrany základních práv osob, jejichž údaje jsou předávány na základě tohoto rozhodnutí – než popis obsahu amerického práva, který Komise předložila.

105 – V tomto smyslu viz rozsudek Schrems (body 74 a 75).

106 – V tomto smyslu viz EDPB, EU-US Privacy Shield – Second Annual Joint Review, ze dne 22. ledna 2019 (s. 17, bod 86).

107 – Viz čl. 45 odst. 5 GDPR. Viz rovněž rozsudek Schrems (bod 76).

108 – Rozhodnutí o „bezpečném přístavu“ tak bylo prohlášeno za neplatné z důvodu, že Komise v uvedeném rozhodnutí neuvedla, že Spojené státy skutečně zajišťují odpovídající úroveň ochrany na základě svých vnitrostátních předpisů nebo mezinárodních závazků (rozsudek Schrems, bod 97). Komise zejména nezjistila existenci pravidel státního charakteru, jež mají omezit případné zásahy do základních práv subjektů údajů (rozsudek Schrems, bod 88), ani účinné právní ochrany před takovými zásahy (rozsudek Schrems, bod 89).

109 – Body 54 až 73 tohoto stanoviska shrnují tato zjištění.

242. Za těchto podmínek posoudím především platnost rozhodnutí o štítu na ochranu soukromí ve světle zjištění učiněných samotnou Komisí ohledně obsahu amerického práva a přezkoumám, zda tato zjištění odůvodňovala přijetí tohoto rozhodnutí o odpovídající úrovni ochrany.

243. V této souvislosti nesouhlasím s názorem, který zastávají DPC a M. Schrems, podle kterého zjištění provedená High Court (Vrchní soud) ve věci práva Spojených států zavazují Soudní dvůr v rámci přezkumu platnosti rozhodnutí o štítu na ochranu soukromí. Posledně uvedený tvrdí, že jelikož zahraniční právo představuje na základě irského procesního práva skutkovou otázku, je ke zjištění jeho obsahu příslušný výlučně předkládající soud.

244. Ustálená judikatura zajisté přiznává vnitrostátnímu soudu výlučnou pravomoc ke zjištění relevantních skutkových okolností, jakož i k výkladu práva členského státu a jeho uplatnění ve sporu, který mu byl předložen¹¹⁰. Tato judikatura odráží rozdělení funkcí mezi Soudním dvorem a předkládajícím soudem v rámci řízení podle článku 267 SFEU. Zatímco pouze Soudní dvůr má pravomoc vykládat unijní právo a rozhodnout o platnosti sekundárního práva, je věcí vnitrostátního soudu, který rozhoduje o konkrétním sporu, jenž mu byl předložen, aby stanovil jeho skutkový a právní kontext k tomu, aby mu Soudní dvůr mohl poskytnout užitečnou odpověď.

245. Důvod existence této výlučné pravomoci předkládajícího soudu se mi nezdá být použitelný na zjištění práva třetí země jakožto skutečnosti, která může ovlivnit závěr Soudního dvora o platnosti aktu sekundárního práva¹¹¹. Vzhledem k tomu, že prohlášení neplatnosti takového aktu je v unijním právním řádu závazné *erga omnes*¹¹², nemůže závěr Soudního dvora záviset na původu žádosti o rozhodnutí o předběžné otázce. Jak přitom zdůraznily společnost Facebook Ireland a vláda Spojených států, pokud by byl Soudní dvůr vázán zjištěními předkládajícího soudu ohledně práva třetího státu, přičemž tato zjištění se mohou lišit v závislosti na vnitrostátním soudu, který je činí, byl by Soudní dvůr na původu žádosti závislý.

246. S přihlédnutím k těmto úvahám mám za to, že pokud odpověď na předběžnou otázku týkající se platnosti unijního aktu předpokládá, že bude posouzen obsah práva třetího státu, není Soudní dvůr, přestože může tento obsah zohlednit, vázán zjištěními učiněnými předkládajícím soudem ohledně práva tohoto třetího státu. Soudní dvůr se od nich může případně odchýlit nebo je doplnit v souladu se zásadou kontradiktornosti s přihlédnutím k dalším zdrojům za účelem zjištění skutečností nezbytných pro posouzení platnosti dotčeného aktu¹¹³.

4) K dosahu standardu „podstatné rovnocennosti“

247. Připomínám, že platnost rozhodnutí o štítu na ochranu soukromí závisí na tom, zda právní řád Spojených států zajišťuje ve prospěch osob, jejichž údaje jsou předávány z Unie do této třetí země, úroveň ochrany, která je „v zásadě rovnocenná“ té, která je zaručena v členských státech na základě GDPR a Listiny, jakož i jejich závazků na základě EÚLP v oblastech vyloučených z působnosti unijního práva.

110 – Viz zejména rozsudky ze dne 4. května 1999, Sürül (C-262/96, EU:C:1999:228, bod 95); ze dne 11. září 2008, Eckelkamp a další (C-11/07, EU:C:2008:489, bod 32), a ze dne 26. října 2016, Senior Home (C-195/15, EU:C:2016:804, bod 20).

111 – V tomto ohledu viz rozsudek Supreme Court (Nejvyšší soud) ze dne 31. května 2019 (bod 6.18).

112 – Viz rozsudek ze dne 13. května 1981, International Chemical Corporation (66/80, EU:C:1981:102, body 12 a 13).

113 – V tomto ohledu viz rozsudek ze dne 22. března 2012, GLS (C-338/10, EU:C:2012:158, body 15, 33 a 34), ve kterém Soudní dvůr za účelem posouzení platnosti nařízení, jež ukládá antidumpingové clo, zohlednil statistiky Eurostatu předložené Komisí na jeho žádost. Viz rovněž rozsudek ze dne 22. října 1991, Nölle (C-16/90, EU:C:1991:402, body 17, 23 a 24). Stejně tak v rozsudku Schrems (bod 90) Soudní dvůr při přezkumu platnosti rozhodnutí o „bezpečném přístavu“ zohlednil některá sdělení Komise.

248. Jak Soudní dvůr zdůraznil v rozsudku ve věci Schrems¹¹⁴, tento standard neznamená, že úroveň ochrany musí být „stejná“ jako úroveň ochrany v Unii. I když se prostředky, které třetí země využívá za účelem ochrany práv subjektů údajů, mohou lišit od prostředků, které stanovuje GDPR vykládané ve světle Listiny, „musí se [...] tyto prostředky v praxi ukázat jako účinné k zajištění ochrany, jež bude v zásadě rovnocenná ochraně zaručené v rámci Unie“.

249. Podle mého názoru z toho rovněž vyplývá, že právo třetího státu určení může odrážet vlastní škálu hodnot, podle které se význam jednotlivých dotčených zájmů může lišit od významu, který je jim přiznán v unijním právním řádu. Ochrana osobních údajů, která panuje v rámci Unie, ostatně odpovídá obzvláště vysokému standardu ve srovnání s úrovní ochrany platnou ve zbytku světa. Kritérium „podstatné rovnocennosti“ proto musí být podle mého názoru použito tak, aby byla zachována určitá pružnost, tak aby byly zohledněny různé právní a kulturní tradice. Splnění tohoto kritéria nicméně znamená, neboť jinak by bylo zbaveno své podstaty, že určité minimální záruky a obecné požadavky na ochranu základních práv, které vyplývají z Listiny a EÚLP, nacházejí svůj ekvivalent v právním řádu třetí země určení¹¹⁵.

250. V tomto ohledu musí být podle čl. 52 odst. 1 Listiny každé omezení výkonu práv a svobod zakotvených Listinou stanoveno zákonem, musí respektovat jejich podstatu a je přípustné pouze tehdy, pokud je za současného dodržení zásady proporcionality nezbytné a skutečně odpovídá cílům obecného zájmu, které uznává Unie, nebo potřebě ochrany práv a svobod druhého. Tyto požadavky v podstatě odpovídají požadavkům stanoveným v čl. 8 odst. 2 EÚLP¹¹⁶.

251. V souladu s čl. 52 odst. 3 Listiny, jelikož práva zaručená články 7, 8 a 47 Listiny odpovídají právům zaručeným články 8 a 13 EÚLP, jsou smysl a rozsah těchto práv stejné, s tím, že unijní právo jim však může poskytnout širší ochranu. Z tohoto hlediska jsou, jak vyplývá z mé analýzy, standardy vyplývající z článků 7, 8 a 47 Listiny, tak jak jsou vyloženy Soudním dvorem, v některých ohledech striktnější než standardy, které vyplývají z článku 8 EÚLP na základě jejich výkladu ze strany Evropského soudu pro lidská práva (dále jen „ESLP“).

252. Rovněž poznamenávám, že věci projednávané před každým z těchto soudů po nich vyžadují, aby přehodnotily určité aspekty své relevantní judikatury. Jednak u dvou nedávných rozsudků ESLP v oblasti dozoru nad elektronickými komunikacemi – a sice rozsudků *Centrum för Rättvisa v. Švédsko*¹¹⁷ a *Big Brother Watch v. Spojené království*¹¹⁸ – došlo k postoupení věci velkému senátu. Kromě toho se tři vnitrostátní soudy obrátily na Soudní dvůr s žádostmi o rozhodnutí o předběžné otázce, které otvírají diskusi o nezbytnosti odchýlení se od judikatury Soudního dvora, která vychází z rozsudku *Tele2 Sverige*¹¹⁹.

253. Po těchto upřesněních nyní přezkoumám platnost rozhodnutí o štítu na ochranu soukromí s ohledem na čl. 45 odst. 1 GDPR vykládaný ve světle Listiny a EÚLP v rozsahu, v němž zaručují jednak práva na respektování soukromého života, jakož i ochranu osobních údajů [oddíl b)], a jednak právo na účinnou soudní ochranu [oddíl c)].

114 – Rozsudek Schrems (body 73 a 74).

115 – V tomto smyslu viz Skupina 29, „Adequacy Referential (updated)“, 28. listopadu 2017, WP 254 (s. 3, 4 a 9).

116 – Článek 8 odst. 2 EÚLP však neodkazuje na pojem „podstata“ práva na respektování soukromého života. V tomto ohledu viz poznámka pod čarou 166 tohoto stanoviska.

117 – ESLP, 19. června 2018 (CE:ECHR:2018:0619JUD003525208, dále jen „rozsudek *Centrum för Rättvisa*“).

118 – ESLP, 13. září 2018 (CE:ECHR:2018:0913JUD005817013, dále jen „rozsudek *Big Brother Watch*“).

119 – Viz věci citované v poznámce pod čarou 102 tohoto stanoviska, jakož i věc C-520/18, *Ordre des barreaux francophones et germanophones* a další (Úř. věst. 2018, C 408, s. 39).

b) K platnosti rozhodnutí o štítu na ochranu soukromí z hlediska práv na respektování soukromého života a ochrany osobních údajů

254. V rámci čtvrté otázky předkládající soud v podstatě zpochybňuje podstatnou rovnocennost mezi úrovní ochrany zajišťovanou ve Spojených státech a úrovní ochrany, kterou mají subjekty údajů v rámci Unie z hlediska svých základních práv na respektování soukromého života a ochranu osobních údajů.

1) K existenci zásahů

255. V bodech 67 až 124 odůvodnění rozhodnutí o štítu na ochranu soukromí Komise uvádí možnost, že veřejné orgány Spojených států budou mít přístup k údajům předaným z Unie a tyto údaje využijí pro účely národní bezpečnosti v rámci programů založených zejména na článku 702 FISA nebo na EO 12333.

256. Provádění těchto programů má za následek neoprávněná vniknutí ze strany amerických zpravodajských služeb, která by byla, pokud by pocházela od orgánů členského státu, považována za zásahy do výkonu práva na respektování soukromého života zaručeného v článku 7 Listiny a v článku 8 EÚLP. Vystavuje subjekty údajů rovněž riziku, že jejich osobní údaje budou předmětem zpracování, které nesplňuje požadavky stanovené v článku 8 Listiny¹²⁰.

257. Bez dalšího je třeba uvést, že práva na respektování soukromého života a ochranu osobních údajů zahrnují ochranu nejen obsahu komunikací, ale i provozních¹²¹ a lokalizačních údajů (společně označovaných výrazem „metadata“). Soudní dvůr i ESLP totiž uznaly, že metadata mohou stejně jako obsahové údaje odhalovat velmi přesné informace týkající soukromí jednotlivce¹²².

258. Podle judikatury Soudního dvora je pro účely prokázání existence zásahu do výkonu práva zaručeného v článku 7 Listiny irrelevantní, zda jsou, či nejsou dotčeny údaje o soukromém životě citlivé nebo zda opatření dozoru mělo, či nemělo pro dotčené osoby případně nepříznivé následky¹²³.

259. Jak již bylo řečeno, sledovací programy založené na článku 702 FISA mají v první řadě za následek zásahy do výkonu základních práv osob, jejichž komunikace odpovídají selektorům vybraným NSA a jsou proto předávány NSA ze strany poskytovatelů služeb elektronických komunikací¹²⁴. Konkrétně povinnost poskytovatelů zpřístupnit údaje agentuře NSA sama o sobě v rozsahu, v němž se odchyluje

120 – I když zpracování může porušovat současně články 7 a 8 Listiny, relevantní rámec pro analýzu pro účely použití článku 8 je systematicky odlišný od rámce, který je spojen s článkem 7. Právo na ochranu osobních údajů znamená podle čl. 8 odst. 2 Listiny, že „[t]yto údaje musí být zpracovány korektně, k přesně stanoveným účelům a na základě souhlasu dotčené osoby nebo na základě jiného oprávněného důvodu stanoveného zákonem“ a že „[k]aždý má právo na přístup k údajům, které o něm byly shromážděny, a má právo na jejich opravu“. Porušení tohoto práva předpokládá, že při zpracování osobních údajů došlo k porušení těchto požadavků. Tak je tomu zejména v případě, kdy zpracování není založeno na souhlasu subjektu údajů, ani na žádném jiném oprávněném důvodu stanoveném zákonem. I když jsou v takové situaci otázky existence zásahu a existence jeho odůvodnění v rámci článku 7 koncepčně odlišné, překrývají se, pokud jde o článek 8 Listiny.

121 – Článek 2 druhý pododstavec písm. b) směrnice 2002/58 vymezuje pojem „provozní údaje“ jako „jakékoli údaje zpracovávané pro účely přenosu sdělení sítí elektronických komunikací nebo pro jeho účtování“.

122 – Viz rozsudek ze dne 8. dubna 2014, Digital Rights Ireland a další (C-293/12 a C-594/12, EU:C:2014:238, dále jen „rozsudek Digital Rights Ireland“, bod 27), a rozsudek Tele2 Sverige (bod 99). Viz rovněž ESLP, 2. srpna 1984, Malone v. Spojené království (CE:ECHR:1984:0802JUD000869179, § 84), a 8. února 2018, Ben Faiza v. Francie (CE:ECHR:2018:0208JUD003144612, § 66).

123 – Viz rozsudek Digital Rights Ireland (bod 33), posudek 1/15 (bod 124), jakož i rozsudek Ministerio Fiscal (bod 51).

124 – Viz body 78 až 81 odůvodnění, jakož i příloha VI bod II rozhodnutí o štítu na ochranu soukromí.

od zásady důvěrnosti komunikací¹²⁵, znamená zásah, i když nejsou později tyto údaje konzultovány a využívány zpravodajskými orgány¹²⁶. *Uchovávání* a účinný *přístup* těchto orgánů k metadatům a obsahu komunikací, které jsou jim dány k dispozici, jakož i *využití* těchto údajů představují další zásahy¹²⁷.

260. Navíc podle zjištění předkládajícího soudu¹²⁸ a jiných zdrojů, jako je zpráva PCLOB o programech prováděných na základě článku 702 FISA, která byla předložena Soudnímu dvoru americkou vládou¹²⁹, v rámci programu Upstream již NSA měla *přístup pro účely jejich filtrování* k rozsáhlým souborům („balíčků“) údajů, které byly součástí komunikačních toků přes „páteřní sítě“ telekomunikací a které zahrnují komunikace, které neobsahují selektory určené NSA. NSA může tyto soubory údajů přezkoumat pouze za účelem rychlého automatizovaného určení, zda obsahují tyto selektory. Pouze takto profiltrované komunikace jsou tak ukládány do databází NSA. Tento přístup k údajům pro účely jejich filtrování tak představuje podle mého názoru rovněž zásah do výkonu práva na respektování soukromého života subjektů údajů bez ohledu na následné využití uložených údajů¹³⁰.

261. Kromě toho zpřístupnění a filtrace dotčených údajů¹³¹, přístup k těmto údajům zpravodajskými orgány, stejně jako jejich případné shromažďování, uchovávání, analýza a využití spadají pod pojem „zpracování“ ve smyslu čl. 4 bodu 2 GDPR a čl. 8 odst. 2 Listiny. Toto zpracování musí být pak v souladu s požadavky stanovenými tímto posledně uvedeným ustanovením¹³².

262. Sledování na základě EO 12333 může zahrnovat přímý přístup k předávaným údajům ze strany zpravodajských orgánů, který s sebou nese zásah do výkonu práva zaručeného v článku 8 EÚLP. K tomuto zásahu se přidává zásah představovaný případným následným využitím těchto údajů.

2) K povaze zásahů „stanovených zákonem“

263. Na základě judikatury Soudního dvora¹³³ a ESLP¹³⁴ platí, že požadavek, že jakýkoliv zásah do výkonu základních práv musí být „stanovený zákonem“ ve smyslu čl. 52 odst. 1 Listiny a čl. 8 odst. 2 EÚLP, znamená nejen, že opatření, které stanoví zásah, musí mít právní základ ve vnitrostátním právu, ale rovněž to, že tento právní základ musí mít určité vlastnosti přístupnosti a předvídatelnosti tak, aby bylo zabráněno riziku svévole.

264. V tomto ohledu se účastníci řízení a zúčastněné strany, které předložily vyjádření Soudnímu dvoru, neshodují v zásadě na tom, zda článek 702 FISA a EO 12333 splňují podmínku předvídatelnosti zákona.

125 – V tomto ohledu viz rozsudek Digital Rights Ireland (bod 32).

126 – V tomto smyslu viz posudek 1/15 (body 124 a 125), ze kterých vyplývá, že sdělení údajů třetí osobě představuje zásah do výkonu základních práv subjektů údajů bez ohledu na jejich následné využití.

127 – V tomto smyslu viz rozsudek Digital Rights Ireland (bod 35), rozsudek Schrems (bod 87) a posudek 1/15 (body 123 až 126).

128 – Viz bod 60 tohoto stanoviska.

129 – PCLOB, Report on the Surveillance Program Operated Pursuant to Section 702 of the [FISA], 2. července 2014 (dále jen „zpráva PCLOB“, s. 84 a 111). Viz rovněž Skupina 29, EU-U. S. Privacy Shield – First Annual Joint Review, 28. listopadu 2017, WP 255 (v B.1.1, s. 15).

130 – Viz poznámka pod čarou 131 tohoto stanoviska.

131 – V tomto ohledu viz bod 222 tohoto stanoviska.

132 – Viz posudek 1/15 (bod 123 a citovaná judikatura).

133 – Viz zejména posudek 1/15 (bod 146).

134 – Viz zejména ESLP, 2. srpna 1984, Malone v. Spojené království (CE:ECHR:1984:0802JUD000869179, § 66), rozhodnutí ze dne 29. června 2006, Weber a Saravia v. Německo (CE:ECHR:2006:0629DEC005493400, dále jen „rozhodnutí Weber a Saravia“, § 84 a citovaná judikatura), jakož i rozsudek ze dne 4. prosince 2015, Zacharov v. Rusko (CE:ECHR:2015:1204JUD004714306, dále jen „rozsudek Zacharov“, § 228).

265. Tato podmínka ve světle výkladu Soudního dvora¹³⁵ a ESLP¹³⁶ vyžaduje, aby právní úprava, která zahrnuje zásah do výkonu práva na respektování soukromého života, stanovila jasná a přesná pravidla pro rozsah a použití dotčeného opatření a uložila minimální požadavky, tak aby osoby, jejichž údaje byly uchovány, měly dostatečné záruky umožňující účinně chránit jejich osobní údaje proti riziku zneužití a proti veškerému neoprávněnému přístupu k údajům a jejich protiprávnímu využívání. Taková pravidla musí zejména stanovit, za jakých okolností a za jakých podmínek mohou veřejné orgány uchovávat údaje, mít k nim přístup a využívat je¹³⁷. Kromě toho sám právní základ, který umožňuje zásah, musí současně vymezit dosah omezení výkonu práva na respektování soukromého života¹³⁸.

266. Stejně jako M. Schrems a EPIC pochybují, že EO 12333, stejně jako PPD 28, která stanoví záruky spojené se všemi zpravodajskými činnostmi týkajícími se přenosu elektromagnetickými prostředky¹³⁹, jsou dostatečně předvídatelné pro to, aby měly „postavení zákona“.

267. Tyto právní předpisy výslovně stanoví, že subjektům práv nepřiznávají soudně vymahatelná práva¹⁴⁰. Subjekty údajů se tedy nemohou dovolávat záruk stanovených PPD 28 před soudy¹⁴¹. Komise se ostatně v rozhodnutí o štítu na ochranu soukromí domnívala, že i když jsou záruky stanovené v této prezidentské směrnicí závazné pro zpravodajské služby¹⁴², „nejsou vyjádřeny právními termíny“¹⁴³. EO 12333 a PPD 28 se spíše podobají vnitřním správním pokynům, které mohou být odvolány nebo změněny prezidentem Spojených států. ESLP přitom již rozhodl, že vnitřní správní směrnice nemají postavení „zákona“¹⁴⁴.

268. Co se týče článku 702 FISA, M. Schrems zpochybňuje předvídatelnost tohoto ustanovení z důvodu, že pro výběr selektorů použitých k filtrování údajů nestanoví dostatečné záruky proti riziku zneužití. Jelikož se tato problematika vztahuje rovněž ke striktně nezbytné povaze zásahů stanovených článkem 702 FISA, přezkoumám ji dále v mém stanovisku¹⁴⁵.

135 – Viz zejména rozsudek Digital Rights Ireland (body 54 a 65), rozsudek Schrems (bod 91), rozsudek Tele2 Sverige (bod 109) a posudek 1/15 (bod 141).

136 – Viz zejména rozhodnutí Weber a Saravia (§ 94 a 95), rozsudek Zacharov (§ 236) a ESLP, 12. ledna 2016, Szabó a Vissy v. Maďarsko (CE:ECHR:2016:0112JUD003713814, dále jen „rozsudek Szabó a Vissy“, § 59).

137 – Viz rozsudek Tele2 Sverige (bod 117) a posudek 1/15 (bod 190). Viz rovněž zejména ESLP, 2. srpna 1984, Malone v. Spojené království (CE:ECHR:1984:0802JUD000869179, § 67); rozsudek Zacharov (§ 229) a rozsudek Szabó a Vissy (§ 62). ESLP zde upřesňuje, že požadavek předvídatelnosti nemá v oblasti odposlechu komunikací stejný dosah jako v jiných oblastech. V kontextu opatření tajného sledování „požadavek předvídatelnosti neznamená, že by jednotlivci měli být s to předvídat, zda a kdy existuje riziko, že jejich komunikace bude orgány odposlouchávána, aby tomu mohli přizpůsobit své chování“.

138 – Posudek 1/15 (bod 139). V tomto smyslu viz rovněž ESLP, 25. března 1983, Silver a další v. Spojené království (CE:ECHR:1983:0325JUD000594772, § 88 a 89).

139 – Body 69 až 77 odůvodnění, jakož i příloha VI bod I rozhodnutí o štítu na ochranu soukromí obsahují popis PPD 28. Je zde upřesněno, že tato prezidentská směrnice se vztahuje na zpravodajské činnosti založené na článku 702 FISA, jakož i na zpravodajské činnosti mimo území Spojených států.

140 – Bod 3.7 písm. c) EO 12333 stanoví: „[t]his order is intended only to improve the internal management of the executive branch and is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity, by any party against the United States, its departments, agencies or entities, its officers, employees, or agents, or any other person“. Článek 6 písm. d) PPD 28 rovněž stanoví: „This directive is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person“.

141 – V tomto smyslu viz EDPB, EU-U. S. Privacy Shield – Second Annual Joint Review, ze dne 22. ledna 2019 (bod 99).

142 – Viz body 69 a 77 odůvodnění rozhodnutí o štítu na ochranu soukromí.

143 – Bod 76 odůvodnění rozhodnutí o štítu na ochranu soukromí.

144 – Viz ESLP, 25. března 1983, Silver a další v. Spojené království (CE:ECHR:1983:0325JUD000594772, § 26 a 86).

145 – Viz body 295 až 301 tohoto stanoviska. V rozsudku Tele2 Sverige (body 116 a 117) a posudku 1/15 (body 140 a 141) byla podmínka předvídatelnosti zákona uvedena jako podmínka bytostně spojená s podmínkou nezbytnosti a přiměřenosti zásahu. Stejně tak podle judikatury ESLP se existence účinných záruk proti rizikům zneužití vztahuje k podmínce „předvídatelnosti“ zásahu i k podmínce týkající se jeho „nezbytnosti v demokratické společnosti“, přičemž dodržení obou těchto podmínek je přezkoumáváno společně. Viz zejména ESLP, 18. května 2010, Kennedy v. Spojené království (CE:ECHR:2010:0518JUD002683905, § 155); rozsudek Zacharov (§ 236), rozsudek Centrum för Rättvisa (§ 107) a rozsudek Big Brother Watch (§ 322).

269. Třetí předběžná otázka zahrnuje problematiku související s dodržováním podmínky týkající se „postavení zákona“. Podstatou této otázky předkládajícího soudu je, zda odpovídající úroveň ochrany zajištěná ve třetí zemi musí být zkoumána pouze s ohledem na právně závazná pravidla v této třetí zemi a zvyklosti, jejichž cílem je zajistit její dodržování, nebo rovněž s ohledem na různé nezávazné nástroje a mimosoudní mechanismy kontroly, které jsou v ní používány.

270. V tomto ohledu čl. 45 odst. 2 písm. a) GDPR uvádí demonstrativní výčet okolností, které musí Komise zohlednit pro účely posouzení odpovídající úrovně ochrany poskytované třetí zemí. Mezi těmito okolnostmi jsou použitelné právní předpisy, jakož i způsob, jakým jsou prováděny. Toto ustanovení rovněž uvádí dopad jiných druhů norem, jako jsou profesní pravidla a bezpečnostní opatření. Vyžaduje mimoto zohlednění „účinných a vymahatelných práv“ a „účinné správní a soudní ochrany pro subjekty údajů, jejichž osobní údaje se předávají“¹⁴⁶.

271. Uvedené ustanovení vykládané jako celek a s ohledem na demonstrativní povahu seznamu, který obsahuje, podle mého názoru znamená, že zvyklosti nebo předpisy, které nejsou založeny na dostupném a předvídatelném právním základě, mohou být zohledněny v rámci celkového posouzení úrovně ochrany zajišťované dotčenou třetí zemí takovým způsobem, aby podpořily záruky, které samy mají právní základ vykazující tyto vlastnosti. Naproti tomu, jak v podstatě tvrdili DPC, M. Schrems, rakouská vláda a EDPB, podobné nástroje nebo zvyklosti nemohou takové záruky nahrazovat, tedy ani samy zajišťovat požadovanou úroveň ochrany.

3) K neexistenci zásahu do podstaty základních práv

272. Požadavek stanovený v čl. 52 odst. 1 Listiny, podle kterého každé omezení výkonu práv a svobod uznaných Listinou musí respektovat podstatu těchto práv, znamená, že pokud zásah podstatu ohrožuje, nemůže jej odůvodnit žádný oprávněný důvod. Zásah je tedy považován za neslučitelný s Listinou, aniž je potřeba zkoumat, zda je způsobilý a nezbytný k dosažení sledovaného cíle.

273. V tomto ohledu Soudní dvůr rozhodl, že vnitrostátní právní úprava, která umožňuje plošný přístup k *obsahu* elektronických komunikací veřejnými orgány, zasahuje do samotné podstaty práva na respektování soukromého života zaručeného v článku 7 Listiny¹⁴⁷. Naopak Soudní dvůr zdůraznil rizika spojená s přístupem a analýzou *provozních a lokalizačních údajů*¹⁴⁸ a rozhodl, že podstata tohoto práva není dotčena, pokud vnitrostátní právní úprava umožňuje plošný přístup státních orgánů k těmto údajům¹⁴⁹.

274. Podle mého názoru nelze mít za to, že článek 702 FISA opravňoval americké zpravodajské orgány k plošnému přístupu k obsahu elektronických komunikací.

275. Přístup k údajům ze strany zpravodajských orgánů na základě článku 702 FISA je totiž *pro účely jejich případné analýzy a jejich využití* omezen na údaje, které splňují selektory, jež jsou spojeny s individuálními cíli.

¹⁴⁶ – Viz rovněž bod 104 odůvodnění GDPR.

¹⁴⁷ – Viz rozsudek Schrems (bod 94). Viz rovněž rozsudky Digital Rights Ireland (bod 39) a Tele2 Sverige (bod 101). Vzhledem k úzké souvislosti mezi právem na respektování soukromého života a právem na ochranu osobních údajů porušuje vnitrostátní opatření, které přiznává veřejným orgánům plošný přístup k obsahu komunikací, podle mého názoru rovněž podstatu práva zakotveného v článku 8 Listiny.

¹⁴⁸ – Viz bod 257 tohoto stanoviska. V rozsudku Tele2 (bod 99) Soudní dvůr zdůraznil, že na základě metadat lze zejména vytvořit profil subjektů údajů. Ve svém stanovisku 04/2014 o dozoru nad elektronickými komunikacemi pro účely zpravodajství a národní bezpečnosti ze dne 10. dubna 2014, WP 215 (s. 5), Skupina 29 uvedla, že z důvodu jejich strukturované povahy je snazší scelit a analyzovat metadata, než obsahové údaje.

¹⁴⁹ – Viz rozsudek Tele2 Sverige (bod 99). Někteří komentátoři si kladli otázku ohledně opodstatněnosti rozlišování mezi plošným přístupem k obsahu komunikací a plošným přístupem k metadatům s ohledem na vývoj technologií a způsobů komunikace. Viz Falot, N. a Hijmans, H., „Tele2: de afweging tussen privacy en veiligheid nader omlijnd“, *Nederlands Tijdschrift voor Europees Recht*, č. 3, 2017 (s. 48), jakož i Ojanen, T., „Making essence of the rights real: the Court of Justice of the European Union clarifies the structure of fundamental rights under the Charter“ (komentář k rozsudku Schrems), *European Constitutional Law Review*, 2016 (s. 5).

276. Kromě toho program Upstream sice může zahrnovat plošný přístup k obsahu elektronických komunikací *za účelem jejich automatizovaného filtrování* v případě, že jsou selektory uplatněny nejen v polích „z“ a „do“, ale rovněž na celý obsah komunikačních toků (vyhledávání „týkající se“ selektoru)¹⁵⁰. Nicméně, jak tvrdí Komise a na rozdíl od toho, co tvrdí M. Schrems a EPIC, dočasný přístup zpravodajských orgánů k celému obsahu elektronických komunikací pouze za účelem jejich filtrování na základě použití selektorů nemůže být postaven naroveň plošnému přístupu k tomuto obsahu¹⁵¹. Podle mého názoru závažnost zásahu, který vyplývá z tohoto časově omezeného přístupu pro účely automatizovaného filtrování, nedosahuje závažnosti zásahu, který vyplývá z plošného přístupu k tomuto obsahu veřejnými orgány za účelem jeho analýzy a případného využití¹⁵². Dočasný přístup za účelem filtrování neumožňuje těmto orgánům, aby uchovály metadata nebo obsah komunikací, které neodpovídají selektorům, ani zejména, jak poznamenala americká vláda, stanovit profily týkajících se jednotlivců, na které se tato kritéria nevztahují.

277. Nicméně to, zda cílení prostřednictvím selektorů v rámci programů založených na článku 702 FISA skutečně omezuje pravomoci zpravodajských orgánů, závisí na rámci pro výběr selektorů¹⁵³. M. Schrems v tomto ohledu tvrdí, že vzhledem k neexistenci dostatečné kontroly za tímto účelem nestanoví americké právo záruku proti plošnému přístupu k obsahu komunikací již ve stadiu filtrování, takže zasahuje do samotné podstaty práva subjektů údajů na respektování soukromého života.

278. Jak uvedu podrobněji dále¹⁵⁴, spíše sdílím tyto pochybnosti ohledně dostatečnosti rámce výběru selektorů pro účely splnění kritérií předvídatelnosti a přiměřenosti zásahů. Existence tohoto rámce, byť nedokonalého, však brání závěru, že článek 702 FISA umožňuje plošný přístup veřejných orgánů k obsahu elektronických komunikací, a je tudíž postaven naroveň zásahu do samotné podstaty zakotveného v článku 7 Listiny.

279. Rovněž zdůrazňuji, že v posudku 1/15 měl Soudní dvůr za to, že podstata práva na ochranu osobních údajů, zaručeného v článku 8 Listiny, je zachována, pokud jsou účely zpracování omezeny a pro zpracování jsou stanovena pravidla, která mají zajistit zejména bezpečnost, důvěrnost a integritu údajů, jakož i chránit je před protiprávním přístupem a zpracováním¹⁵⁵.

150 – Viz poznámka pod čarou 87 rozhodnutí o štitu na ochranu soukromí. Nicméně podle vyjádření EPIC a písemné odpovědi vlády Spojených států na otázky položené Soudním dvorem Soud pro uplatňování zákona FISA v roce 2017 rozhodl o pozastavení vyhledávání „týkajícího se“ selektorů z důvodu vad, které se týkaly vyhledávání tohoto druhu. Kongres nicméně v aktu o opětovném povolení FISA přijatém v roce 2018 stanovil možnost opětovně zavést tento druh vyhledávání se souhlasem Soudu pro uplatňování zákona FISA a Kongresu. Viz rovněž EDPB, EU-U. S. Privacy Shield – Second Annual Joint Review, 22. ledna 2019 (s. 27, bod 55).

151 – Z tohoto hlediska předkládající soud v bodech 188 a 189 svého rozsudku ze dne 3. října 2017 odlišuje hromadné vyhledávání od hromadného získávání, shromažďování nebo uchovávání. Tento soud má v podstatě za to, že jestliže program Upstream implikuje hromadné vyhledávání v rámci všech toků údajů přenášených „páteřními sítěmi“ telekomunikací, jsou získávání, shromažďování a uchovávání zacíleny v tom smyslu, že jejich předmětem jsou pouze údaje, které obsahují dotčené selektory.

152 – V tomto smyslu viz rozsudek Supreme Court (Nejvyšší soud) ze dne 31. května 2019 (body 11.2 a 11.3). Daný soud v něm uvádí: „[I]t is inevitable that any screening process designed to identify data of interest will necessarily involve all of the data available, for the whole bod of the screening process is to identify within that entire universe of available data the relevant material which may be of interest and thus require closer scrutiny. Perhaps part of the problem lies in the fact that the term ‚processing‘ covers a wide range of activity, apparently, in the view of the DPC, including screening. On the assumption that is a correct view of the law, then it is technically correct to describe bulk screening as involving indiscriminate processing. But the use of that terminology might be taken to imply that other forms of processing, which are significantly more invasive, are carried out on an indiscriminate basis“.

153 – Viz posudek 1/15 (bod 122). Viz rovněž zpráva Evropské komise pro demokracii prostřednictvím práva (Benátská komise) o demokratické kontrole agentur pro shromažďování signálových zpravodajských informací ze dne 15. prosince 2015, studie č. 719/2013 [CDL-AD(2015)011, s. 11]: „V praxi znamená otázka, zda tento postup náležitě omezuje nadbytečné neoprávněné přístupy k nevinné osobní komunikaci, zjistit, zda je selektor dostatečně relevantní a konkrétní a zda je dostatečná kvalita algoritmu programu používaného pro identifikaci relevantních údajů v rámci zvolených parametrů [...]“.

154 – Viz body 297 až 301 tohoto stanoviska.

155 – Posudek 1/15 (bod 150).

280. V rozhodnutí o štítu na ochranu soukromí Komise konstatovala, že článek 702 FISA i PPD 28 vymezují účely, pro které lze údaje shromažďovat v rámci programů prováděných na základě článku 702 FISA¹⁵⁶. Komise v něm rovněž uvedla, že PPD 28 stanoví pravidla, která vymezují přístup k údajům, jakož i ukládání a jejich zpřístupnění, tak aby byla zajištěna jejich bezpečnost a ochrana před neoprávněným přístupem¹⁵⁷. Jak ukáže další část mého pojednání¹⁵⁸, mám pochybnosti zejména o tom, zda jsou účely dotčených zpracování vymezeny dostatečně jasně a přesně, aby byla zajištěna úroveň ochrany v zásadě rovnocenná úrovni ochrany, která panuje v unijním právním řádu. Tyto případné nedostatky však podle mého názoru nestačí k tomu, aby umožnily zjištění, že by podobné programy porušovaly podstatu práva na ochranu osobních údajů, pokud by byly realizovány v rámci Unie.

281. Kromě toho připomínám, že odpovídající úroveň ochrany zajištěná v rámci sledování na základě EO 12333 musí být posuzována z hlediska ustanovení EÚLP. V tomto ohledu z rozhodnutí o štítu na ochranu soukromí vyplývá, že jedinými omezeními provádění opatření založených na EO 12333 ke shromažďování údajů týkajících se neamerických osob jsou omezení, která stanoví PPD 28¹⁵⁹. Tato prezidentská směrnice stanoví, že používání zahraničního zpravodajství musí být „v nejvyšší možné míře uzpůsobeno na míru“. Uvádí nicméně výslovně možnost shromáždit údaje „hromadně“ mimo americké území pro účely sledování určitých konkrétních cílů národní bezpečnosti¹⁶⁰. Podle názoru M. Schremse ustanovení PPD 28, která ostatně nezakládá práva jednotlivců, nechrání subjekty údajů před rizikem plošného přístupu k obsahu jejich elektronických komunikací.

282. V tomto ohledu se omezím na to, že ESLP ve své judikatuře týkající se článku 8 EÚLP nepoužil pojem „zásah do podstaty nebo do samotné podstaty práva na respektování soukromého života“¹⁶¹. Tento soud se doposud nedomníval, že by režimy umožňující odposlechy elektronických komunikací, byť rozsáhlé, *přesahovaly jako takové prostor pro volné uvážení členských států*. ESLP se domnívá, že takové režimy jsou slučitelné s čl. 8 odst. 2 EÚLP, pokud jsou spojeny s určitými minimálními zárukami¹⁶². Za těchto podmínek nepovažuji za vhodné dospět k závěru, že takový režim sledování, jaký je stanoven v EO 12333, překračuje prostor pro volné uvážení členských států, aniž by byl proveden jakýkoliv přezkum případných záruk, které jsou s ním spojeny.

156 – Viz body 70, 103 a 109 odůvodnění rozhodnutí o štítu na ochranu soukromí.

157 – Viz body 83 až 87 odůvodnění, jakož i příloha VI bod I písm. c) rozhodnutí o štítu na ochranu soukromí. Podotýkám, že podle zprávy PCLOB (s. 51 až 66) se postupy „minimalizace“ NSA na základě článku 702 FISA týkají u většiny jejich aspektů pouze amerických osob. PPD 28 měla za cíl rozšířit použitelné záruky na neamerické osoby. Viz PCLOB, Report to the President on the Implementation of [PPD 28]: Signals Intelligence Activities, dostupná na adrese [https://www.pclob.gov/reports/report-PPD28/\(s. 2\)](https://www.pclob.gov/reports/report-PPD28/(s.2)). Ukládání a využívání údajů pro účely národní bezpečnosti poté, co byly získány veřejnými orgány, však podle mého názoru nespádá do působnosti unijního práva (viz bod 226 tohoto stanoviska). Odpovídající úroveň ochrany zajištěná v rámci těchto činností tedy musí být posuzována pouze s ohledem na článek 8 EÚLP.

158 – Viz body 283 až 289 tohoto stanoviska.

159 – Komise konkrétně v bodě 127 odůvodnění rozhodnutí o štítu na ochranu soukromí konstatovala, že čtvrtý dodatek Ústavy Spojených států se nevztahuje na neamerické osoby.

160 – Viz body 73 a 74 odůvodnění, jakož i příloha VI bod I písm. b) rozhodnutí o štítu na ochranu soukromí. Tyto cíle zahrnují boj proti špiónáži a proti jiným hrozbám a činnostem vedeným zahraničními mocnostmi proti Spojeným státům a jeho zájmům; proti teroristickým hrozbám; proti hrozbám plynoucím z vývoje, držení, šíření nebo používání zbraní hromadného ničení; proti hrozbám spojeným s kybernetickou bezpečností; proti hrozbám pro ozbrojené síly Spojených států nebo jeho spojenců a proti hrozbám přeshraniční trestné činnosti. Podle poznámky pod čarou 5 PPD 28 se omezení cílů odůvodňujících použití hromadně shromažďovaných údajů nepoužije, pokud je takové shromažďování pouze dočasné a s cílem usnadnit cílené shromažďování.

161 – I když ustanovení EÚLP nezmiňují „podstatu“ základních práv, rovnocenný pojem „samotná podstata“ základního práva se nachází v judikatuře ESLP týkající se některých jejích ustanovení. Ohledně samotné podstaty práva na spravedlivý proces zaručeného v článku 6 EÚLP viz zejména ESLP, 25. května 1985, Ashingdane v. Spojené království (CE:ECHR:1985:0528JUD000822578, § 57 a 59); 21. prosince 2000, Heaney and McGuinness v. Irsko (CE:ECHR:2000:1221JUD003472097, § 55 a 58), a 23. června 2016, Baka v. Maďarsko (CE:ECHR:2016:0623JUD002026112, § 121). Ohledně samotné podstaty práva uzavřít manželství zakotveného v článku 12 EÚLP, viz ESLP, 11. července 2002, Christine Goodwin v. Spojené království (CE:ECHR:2002:0711JUD002895795, § 99 a 101). Ohledně samotné podstaty práva na vzdělání zaručeného v článku 2 Protokolu č. 1 k EÚLP, viz ESLP, 23. července 1968, věc „týkající se některých aspektů jazykového režimu vzdělávání v Belgii“ (CE:ECHR:1968:0723JUD000147462, § 5).

162 – Viz zejména rozsudky Centrum för Rättvisa (§ 112 až 114, jakož i citovaná judikatura) a Big Brother Watch (§ 337).

4) Ke sledování oprávněného cíle

283. Podle čl. 52 odst. 1 Listiny musí každé omezení výkonu práv a svobod uznaných touto listinou skutečně odpovídat cílům obecného zájmu, které uznává Unie. Článek 8 odst. 2 Listiny rovněž stanoví, že jakékoliv zpracování osobních údajů, které není založeno na souhlasu dotčené osoby, musí být založeno na „oprávněném důvodu stanoveném zákonem“. Článek 8 odst. 2 EÚLP obsahuje výčet cílů, které mohou odůvodnit zásah do výkonu práva na respektování soukromého života.

284. Na základě rozhodnutí o štítu na ochranu soukromí může být přistoupení k zásadám, které stanoví, omezeno tak, aby splňovalo povinnosti týkající se národní bezpečnosti, veřejného zájmu a dodržování právních předpisů¹⁶³. Body 67 až 124 odůvodnění tohoto rozhodnutí konkrétněji přezkoumávají omezení, která vyplývají z přístupu k údajům a jejich využívání americkými veřejnými orgány pro účely národní bezpečnosti.

285. Je nesporné, že ochrana národní bezpečnosti je oprávněným cílem, který může odůvodnit výjimky z požadavků GDPR¹⁶⁴, jakož i základních práv zakotvených v článcích 7 a 8 Listiny¹⁶⁵ a v čl. 8 odst. 2 EÚLP. M. Schrems, rakouská vláda a EPIC však poukázali na to, že cíle sledované v rámci sledovacích programů založených na článku 702 FISA a EO 12333 přesahují pouhou národní bezpečnost. Předmětem těchto nástrojů je totiž získání „zahraničního zpravodajství“, přičemž tento pojem se vztahuje na různé druhy informací, které zahrnují informace týkající se národní bezpečnosti, aniž jsou na ně nutně omezeny¹⁶⁶. Pod pojem „zahraniční zpravodajství“ ve smyslu článku 702 FISA tedy spadají údaje týkající řízení zahraničních věcí¹⁶⁷. EO 12333 vymezuje tento pojem tak, že zahrnuje informace o kapacitách, záměrech nebo činnostech zahraničních vlád, zahraničních organizací a zahraničních osob¹⁶⁸. M. Schrems zpochybňuje oprávněnost takto sledovaného, jelikož přesahuje národní bezpečnost.

286. Podle mého názoru může oblast bezpečnosti státu do určité míry zahrnovat ochranu zájmů souvisejících s řízením zahraničních věcí¹⁶⁹. Kromě toho není nemyšlitelné, že některé jiné cíle, než je ochrana národní bezpečnosti, které zahrnuje pojem „zahraniční zpravodajství“, jak je vymezen v článku 702 FISA a v EO 12333, odpovídají významným cílům veřejného zájmu, které mohou odůvodnit zásah do základních práv na respektování soukromého života a ochranu osobních údajů. Tyto cíle by byly v každém případě méně zatěžující v rámci zvážení základních práv subjektů údajů a cíle sledovaného zásahem¹⁷⁰.

163 – Viz bod 197 tohoto stanoviska.

164 – Viz čl. 23 odst. 1 písm. a) GDPR.

165 – Viz rozsudek Schrems (bod 88). Soudní dvůr považoval příbuzný pojem „veřejná bezpečnost“ ve smyslu ustanovení SFEU, která povolují odchylky od základních svobod, které tato zaručuje, za autonomní pojem unijního práva, který zahrnuje vnitřní i vnější bezpečnost členských států [viz zejména rozsudky ze dne 26. října 1999, Sirdar (C-273/97, EU:C:1999:523, bod 17), jakož i ze dne 13. září 2016, CS (C-304/14, EU:C:2016:674, bod 39 a citovaná judikatura)]. Zatímco vnitřní bezpečnost může být ohrožena zejména přímou hrozbou pro klid a fyzickou bezpečnost obyvatel dotčeného členského státu, vnější bezpečnost může být ohrožena zejména z důvodu rizika vážného narušení vnějších vztahů nebo poklidného soužití lidí. Aniž by bylo možné jednostranně určit obsah těchto pojmů, každý členský stát má určitý prostor pro uvážení za účelem vymezení svých základních zájmů v oblasti bezpečnosti. Viz zejména rozsudek ze dne 2. května 2018, K. a H. F. (Právo pobytu a obvinění z válečných zločinů) (C-331/16 a C-366/16, EU:C:2018:296, body 40 až 42, jakož i citovaná judikatura). Tyto úvahy jsou podle mého názoru použitelné na výklad pojmu „národní bezpečnost“ jakožto zájmu, jehož ochrana může odůvodňovat omezení ustanovení GDPR a práv zaručených v článcích 7 a 8 Listiny.

166 – V tomto ohledu viz bod 89 odůvodnění a poznámka pod čarou 97 rozhodnutí o štítu na ochranu soukromí.

167 – Viz bod 55 tohoto stanoviska.

168 – Viz bod 61 tohoto stanoviska.

169 – V rozsudku Centrium för Rättvisa (§ 111) ELP rozhodl, že sledování, které má za cíl podpořit zahraniční, obrannou a bezpečnostní politiku Švédska, jakož i odhalování organizovaných vnějších hrozeb ve Švédsku, sledovalo oprávněné cíle týkající se národní bezpečnosti.

170 – V tomto ohledu viz rozsudky Tele2 Sverige (bod 115) a Ministerio Fiscal (bod 55). V těchto rozsudcích Soudní dvůr zdůraznil vztah mezi stupněm závažnosti zásahu a důležitostmi zájmu, kterým se tento zásah odůvodňuje.

287. V souladu s čl. 52 odst. 1 Listiny je však ještě třeba, aby byly národní bezpečnost nebo jiný legitimní cíl opatřeními upravujícími dotčené zásahy skutečně sledovány¹⁷¹. Kromě toho cíle zásahů musí být definovány tak, aby splňovaly požadavky jasnosti a přesnosti¹⁷².

288. Podle M. Schremse přitom účel sledování stanovených článkem 702 FISA a EO 12333 není uveden dostatečně přesně k tomu, aby splňoval záruky předvídatelnosti a přiměřenosti. Tak je tomu zejména proto, že tyto předpisy definují pojem „zahraniční zpravodajství“ zvláště široce. Navíc Komise v bodě 109 odůvodnění rozhodnutí o štítu na ochranu soukromí konstatovala, že článek 702 FISA vyžaduje, aby shromažďování informací v oblasti zahraničního zpravodajství představovalo „důležitý účel“ shromažďování, přičemž tato formulace *prima facie*, a jak uvedl EPIC, nevylučuje sledování dalších neurčených cílů.

289. Z těchto důvodů, aniž je vyloučeno, že sledování na základě článku 702 FISA nebo EO 12333 odpovídají oprávněným cílům, je možné si položit otázku, zda jsou tyto cíle vymezeny natolik dostatečně jasně a přesně, aby bylo zabráněno riziku zneužití a byl umožněn přezkum přiměřenosti zásahů, které z nich vyplývají¹⁷³.

5) K nezbytnosti a přiměřenosti zásahů

290. Soudní dvůr opakovaně zdůraznil, že práva zakotvená v člancích 7 a 8 Listiny nepředstavují absolutní výsady, ale musí být posuzována v souvislosti se svou funkcí ve společnosti a v souladu se zásadou proporcionality vyvážená s ostatními základními právy¹⁷⁴. Jak zdůraznila společnost Facebook Ireland, mezi tato jiná práva patří i právo na bezpečnost zaručené v článku 6 Listiny.

291. V tomto ohledu podle ustálené judikatury platí, že jakýkoli zásah do výkonu práv zaručených v člancích 7 a 8 Listiny musí být předmětem striktní kontroly přiměřenosti¹⁷⁵.

292. Z rozsudku Schrems zejména vyplývá, že „na naprosto nezbytné se tedy neomezuje taková právní úprava, která globálně dovoluje uchovávat všechny osobní údaje [...] bez jakéhokoli rozlišení, omezení nebo výjimky činěných v závislosti na sledovaném cíli a bez stanovení objektivního kritéria umožňujícího vymezit přístup veřejných orgánů k údajům a jejich následné využití pro konkrétní účely, striktně omezené a způsobilé odůvodnit zásah způsobený jak přístupem k těmto údajům, tak jejich využíváním“¹⁷⁶.

293. Soudní dvůr rovněž rozhodl, že s výjimkou řádně odůvodněných případů naléhavosti musí přístup podléhat předběžné kontrole ze strany soudu nebo nezávislého správního orgánu, jehož rozhodnutí má za cíl omezit přístup k údajům a jejich následné využití na to, co je naprosto nezbytné pro účely dosažení sledovaného cíle¹⁷⁷.

171 – Skupina 29 ve svém pracovním dokumentu o sledování elektronických komunikací pro účely zpravodajství a národní bezpečnosti ze dne 5. prosince 2014, WP 228 (s. 27), zdůraznila význam kritického posouzení, zda je sledování skutečně prováděno pro účely národní bezpečnosti.

172 – Viz posudek 1/15 (bod 181), ve kterém Soudní dvůr rozhodl, že znění zákonných ustanovení upravujících zásahy nesplňuje požadavky na jasnost a přesnost, takže tyto zásahy nejsou omezeny na to, co je nezbytně nutné. V témže smyslu měl generální advokát Y. Bot ve svém stanovisku ve věci Schrems (C-362/14, EU:C:2015:627, body 181 až 184) za to, že cíle sledovacích opatření byly formulovány příliš široce na to, aby byly považovány za cíle obecného zájmu, s výjimkou národní bezpečnosti.

173 – Podobné pochybnosti byly vyjádřeny EIOÚ v jeho stanovisku 4/2016 týkajícím se „štítu na ochranu soukromí EU-USA“ (Privacy Shield) – Návrh na rozhodnutí o odpovídající úrovni ochrany ze dne 30. května 2016 (s. 8).

174 – Viz rozsudek ze dne 9. listopadu 2010, Volker und Markus Schecke a Eifert (C-92/09 a C-93/09, EU:C:2010:662, bod 48); posudek 1/15 (bod 136), a rozsudek ze dne 24. září 2019, Google (Územní dosah práva na odstranění důkazů) (C-507/17, EU:C:2019:772, bod 60).

175 – Viz zejména rozsudek ze dne 16. prosince 2008, Satakunnan Markkinapörssi a Satamedia (C-73/07, EU:C:2008:727, bod 56), rozsudek Digital Rights Ireland (body 48 a 52), rozsudek Schrems (body 78 a 92), jakož i posudek 1/15 (body 139 a 140). Viz rovněž bod 140 odůvodnění rozhodnutí o štítu na ochranu soukromí.

176 – Rozsudek Schrems (bod 93). V tomto smyslu viz rovněž rozsudek Digital Rights Ireland (bod 60).

177 – Viz rozsudek Tele2 Sverige (bod 120) a posudek 1/15 (bod 202).

294. V článku 23 odst. 2 GDPR je nyní uvedena řada záruk, které musí členský stát stanovit, pokud se od ustanovení tohoto nařízení odchyľuje. Právní úprava umožňující takovou odchylku musí obsahovat ustanovení týkající se zejména účelů zpracování, rozsahu odchylky, záruk proti zneužití, doby uchovávání, jakož i práva subjektů údajů být informovány o odchylce, pokud toto informování nemůže být na újmu účelu odchylky.

295. V projednávané věci M. Schrems tvrdí, že článek 702 FISA není spojen s dostatečnými zárukami proti riziku zneužití a neoprávněného přístupu k údajům. Zejména není dostatečně vymezen výběr selektorů, takže toto ustanovení neposkytuje zajištění proti plošnému přístupu k obsahu komunikací.

296. Vláda Spojených států a Komise naopak tvrdí, že článek 702 FISA omezuje výběr selektorů objektivními kritérii, jelikož toto ustanovení umožňuje výhradně shromažďování údajů o elektronických komunikacích neamerických osob, které se nacházejí mimo území Spojených států, za účelem získání informací v oblasti zahraničního zpravodajství.

297. Podle mého názoru lze pochybovat o dostatečně jasném a přesném charakteru těchto kritérií, jakož i o existenci dostatečných záruk pro předcházení riziku zneužití.

298. Nejprve bod 109 odůvodnění rozhodnutí o štítu na ochranu soukromí stanoví, že selektory nejsou před jejich uplatněním jednotlivě schvalovány Soudem pro uplatňování zákona FISA, ani jiným soudním či nezávislým správním orgánem. Komise v něm konstatovala, že „Soud pro uplatňování zákona FISA nepovoluje jednotlivá sledovací opatření, nýbrž povoluje celé sledovací programy [...], a to na základě ročních osvědčení“, což vláda Spojených států potvrdila před Soudním dvorem. Uvedený bod odůvodnění stanoví, že „osvědčení, která Soud pro uplatňování zákona FISA schvaluje, neobsahují žádné informace o jednotlivých osobách, které jsou předmětem cíleného sledování, nýbrž jen identifikují kategorie zahraničních zpravodajských informací“, které lze shromažďovat. Komise v něm rovněž konstatuje, že „Soud pro uplatňování zákona FISA nezjišťuje – podle principu důvodného podezření či jiného principu – zda jsou za účelem získání zahraničních zpravodajských informací fyzické osoby cíleny správně“, kontroluje však podmínku, že „důležitým účelem získávání informací je získání zahraničních zpravodajských informací“.

299. Dále podle uvedeného bodu odůvodnění článek 702 FISA opravňuje NSA ke shromažďování komunikací „jen tehdy, lze-li se důvodně domnívat, že předmětný způsob komunikace je používán k předávání zahraničních zpravodajských informací“. Bod 70 odůvodnění rozhodnutí o štítu na ochranu soukromí doplňuje, že určování selektorů probíhá v zastřešujícím „rámci priorit národního zpravodajství“ (National Intelligence Priorities Framework, NIPF). Toto rozhodnutí nestanoví přesnější požadavky odůvodnění či opodstatnění výběru selektorů s ohledem na správné priority, které musí respektovat NSA¹⁷⁸.

300. Konečně bod 71 odůvodnění rozhodnutí o štítu na ochranu soukromí odkazuje na požadavek stanovený v PPD 28, podle kterého musí sběr zpravodajských informací být „v nejvyšší možné míře uzpůsoben na míru“. Mimo skutečnost, že tato prezidentská směrnice nezakládá práva jednotlivců, podstatnou rovnocennost mezi kritériem činnosti „v nejvyšší možné míře uzpůsobené na míru“ a kritériem „striktní nezbytnosti“, které čl. 52 odst. 1 Listiny ukládá pro účely odůvodnění zásahu do výkonu práv zaručených v člancích 7 a 8 Listiny, zdaleka nepovažuji za zjevnou¹⁷⁹.

178 – Zpráva PCLOB (s. 45) uvádí: „With respect to the foreign intelligence purpose, the NSA targeting procedures require the analyst only to ‚identify‘ the foreign power or foreign territory regarding which the foreign intelligence information is to be acquired. By policy, but not as a requirement of the targeting procedures, the NSA also requires that all taskings be accompanied by a very brief statement (typically no more than one sentence long) that further explains the analyst’s rationale for assessing that tasking the selector in question will result in the acquisition of the types of foreign intelligence information authorized by the Section 702 certification“.

179 – V tomto smyslu viz Skupina 29, Opinion 1/2016 on the EU-U. S. Privacy Shield draft adequacy decision, 13. dubna 2016, WP 238 (v 3.3.1, s. 38); usnesení Parlamentu ze dne 6. dubna 2017 o přiměřenosti ochrany poskytované štítem EU – USA na ochranu soukromí, P8_TA(2017)0131 (bod 17), jakož i zpráva Parlamentu o dopadech dat velkého objemu na základní práva: soukromí, ochrana údajů, zákaz diskriminace, bezpečnost a prosazování práva ze dne 20. února 2017, A8-0044/2017 (bod 17).

301. S přihlédnutím k těmto úvahám není jisté, že na základě skutečností uvedených v rozhodnutí o štítu na ochranu soukromí je sledování založené na článku 702 FISA spojeno se zárukami týkajícími se omezení osob, které mohou být předmětem sledování, a cílů, pro které mohou být údaje shromažďovány, v zásadě rovnocenné zárukám, které jsou vyžadovány na základě GDPR vykládaného ve světle článků 7 a 8 Listiny¹⁸⁰.

302. Kromě toho ohledně posouzení odpovídající úrovně ochrany sledování na základě EO 12333 přiznává ESLP členským státům široký prostor pro volné uvážení, pokud jde o volbu prostředků k ochraně jejich národní bezpečnosti, avšak tento prostor je omezen požadavkem na stanovení vhodných a dostatečných záruk proti zneužití¹⁸¹. ESLP ve své judikatuře týkající se tajného sledování přezkoumává, zda vnitrostátní právo, o které se tato opatření opírají, obsahuje dostatečné a účinné záruky a ochranná opatření, které jsou vhodné ke splnění požadavků „předvídatelnosti“ a „nezbytnosti v demokratické společnosti“¹⁸².

303. ESLP v tomto ohledu stanoví několik minimálních záruk. Tyto záruky se týkají jasného uvedení povahy trestných činů, které mohou vést k vydání příkazu k odposlechu, vymezení kategorií osob, jejichž komunikace mohou být odposlouchávány, stanovení maximální doby trvání provádění opatření, postupu, který je třeba dodržet při přezkumu, používání a uchovávání shromážděných údajů, opatření, která mají být přijata za účelem sdělování údajů dalším stranám, a okolností, za kterých může nebo musí dojít k výmazu nebo ke zničení záznamů¹⁸³.

304. Vhodnost a účinnost záruk, které vymezují zásah, závisí na všech okolnostech dané věci, včetně povahy, rozsahu a doby trvání opatření, důvodů požadovaných pro jejich nařízení, orgánů příslušných k jejich přijetí, provedení a kontrole a druhu opravného prostředku stanoveného vnitrostátním právem¹⁸⁴.

305. Pro účely posouzení odůvodnění tajného sledování ESLP zejména zohledňuje všechny kontroly prováděné „v okamžiku, kdy je nařízeno“, „během doby, kdy se koná“, a „poté, co bylo ukončeno“¹⁸⁵. Pokud jde o první z těchto tří fází, ESLP vyžaduje, aby takové opatření bylo povoleno nezávislým orgánem. I když soudní pravomoc podle něj představuje nejlepší záruky nezávislosti, nestrannosti a legality řízení, dotčený orgán nemusí nutně spadat do soudnictví¹⁸⁶. Důkladný soudní přezkum v pozdější fázi může vyvážit případné nedostatky povolovacího řízení¹⁸⁷.

306. V projednávané věci z rozhodnutí o štítu na ochranu soukromí vyplývá, že jediné záruky, které omezují shromažďování a využívání údajů mimo území Spojených států, jsou obsaženy v PPD 28, jelikož článek 702 FISA se mimo toto území nepoužije. Nejsem přesvědčen o tom, že by tyto záruky mohly stačit ke splnění podmínek „předvídatelnosti“ a „nezbytnosti v demokratické společnosti“.

180 – V tomto smyslu viz Skupina 29, EU-U. S. Privacy Shield – First Annual Joint Review, 28. listopadu 2017, WP 255 (s. 3); usnesení Evropského parlamentu ze dne 5. července 2018 o přiměřenosti ochrany poskytované štítem EU – USA na ochranu soukromí, P8_TA(2018)0315 (bod 22), a EDPB, EU-U. S. Privacy Shield – Second Annual Joint Review, 22. ledna 2019 (body 81 až 83 a 87).

181 – Viz zejména rozsudky Zacharov (§ 232) a Szabó a Vissy (§ 57).

182 – Viz zejména rozsudky Zacharov (§ 237), Centrium för Rättvisa (§ 111) a Big Brother Watch (§ 322).

183 – Viz zejména rozhodnutí Weber a Saravia (§ 95); ESLP, 28. června 2007, Asociace pro evropskou integraci a lidská práva a Ekimdzhev (CE:ECHR:2007:0628JUD006254000, § 76), jakož i rozsudek Zacharov (§ 231).

184 – Viz zejména rozhodnutí Weber a Saravia (§ 106), rozsudek Zacharov (§ 232) a rozsudek Centrium för Rättvisa (§ 104).

185 – Viz zejména ESLP, 6. září 1978, Klass a další v. Německo (CE:ECHR:1978:0906JUD000502971, § 55), rozsudek Zacharov (§ 233), jakož i rozsudek Centrium för Rättvisa (§ 105).

186 – Viz zejména rozsudek Klass (§ 56); ESLP, 18. května 2010, Kennedy v. Spojené království (CE:ECHR:2010:0518JUD002683905, § 167), jakož i rozsudek Zacharov (§ 233 a 258).

187 – Viz rozsudky Szabó a Vissy (§ 77) a Centrium för Rättvisa (§ 133).

307. Předně jsem již uvedl, že tato prezidentská směrnice nezakládá práva jednotlivců. Dále pochybuji o tom, že požadavek zajistit sledování „v nejvyšší možné míře uzpůsobené na míru“ je formulován dostatečně jasně a přesně k tomu, aby byly subjekty údajů odpovídajícím způsobem chráněny před riziky zneužití¹⁸⁸. Konečně, rozhodnutí o štítu na ochranu soukromí nestanoví, že sledování na základě EO 12333 podléhá předchozí kontrole ze strany nezávislého orgánu nebo že může být předmětem soudního přezkumu *a posteriori*¹⁸⁹.

308. Za těchto podmínek si kladu otázku ohledně opodstatněnosti zjištění, podle kterého Spojené státy zajišťují v rámci činností jejich zpravodajských služeb na základě článku 702 FISA a EO 12333 odpovídající úroveň ochrany ve smyslu čl. 45 odst. 1 GDPR vykládaného ve světle článků 7 a 8 Listiny, jakož i článku 8 EÚLP.

c) K platnosti rozhodnutí o štítu na ochranu soukromí s ohledem na právo na účinnou právní ochranu

309. Pátou předběžnou otázkou je Soudní dvůr vyzván k tomu, aby určil, zda subjekty, jejichž údaje jsou předávány do Spojených států, požívají ve Spojených státech soudní ochrany v podstatě rovnocenné soudní ochraně, která musí být zajištěna v Unii na základě článku 47 Listiny. Podstatou desáté otázky předkládajícího soudu je, zda je třeba na pátou otázku zodpovědět kladně vzhledem k zavedení mechanismu ombudsmana v rozhodnutí o štítu na ochranu soukromí.

310. Bez dalšího konstatuji, že v bodě 115 odůvodnění tohoto rozhodnutí Komise uznává, že americký právní systém obsahuje mezery v soudní ochraně jednotlivců.

311. Podle tohoto bodu odůvodnění se zaprvé „přinejmenším některých z právních základů, které zpravodajské orgány USA mohou využít (např. EO 12223)“, možnosti soudní nápravy netýkají. EO 12333 a PPD 28 totiž nepřiznávají práva subjektům údajů a subjekty údajů se jich nemohou dovolávat před soudy. Účinná soudní ochrana přitom předpokládá přinejmenším to, že jednotlivci mají práva, kterých se lze dovolávat před soudem.

312. Zadruhé „i tehdy, pokud pro osoby, které nejsou osobami USA, možnosti nápravy v zásadě existují, např. u sledování podle zákona FISA, jsou dostupné právní kroky omezené a nároky vznesené [...] osobami, které neprokáží ‚aktivní legitimaci‘, budou prohlášeny za nepřípustné, což omezuje přístup k běžným soudům“.

313. Z bodů 116 až 124 odůvodnění rozhodnutí o štítu na ochranu soukromí vyplývá, že zavedení ombudsmana má za cíl tato omezení kompenzovat. V bodě 139 odůvodnění tohoto rozhodnutí Komise dospívá k závěru, že „*dohlížecí a odvolací* mechanismy poskytované štítem na ochranu soukromí *jako celek* [...] poskytují subjektu údajů procesní prostředky, které mu umožní získat přístup k osobním údajům, které se jej týkají, a v konečném důsledku dosáhnout opravy nebo výmazu takových údajů“ (kurzivou zvýraznil autor stanoviska).

314. Připomenu obecné zásady, které vyplývají z judikatury Soudního dvora a ESLP týkající se prostředků nápravy před soudem proti opatřením týkajícím se sledování komunikací, a přezkoumám, zda opravné prostředky stanovené americkým právem, jak jsou popsány v rozhodnutí o štítu na ochranu soukromí, umožňují zajistit odpovídající soudní ochranu subjektů údajů [oddíl 1)]. Následně určím, zda zavedení mimosoudního mechanismu ombudsmana v případě potřeby umožňuje zaplnit případné mezery, kterými se vyznačuje soudní ochrana těchto subjektů [oddíl 2)].

188 – Je tomu tak tím spíše, přihlédneme-li k úvahám uvedeným v bodě 281 tohoto stanoviska.

189 – Viz body 330 a 331 tohoto stanoviska.

1) K účinnosti právem USA stanovených prostředků nápravy před soudem

315. Zaprvé čl. 47 první pododstavec Listiny zakotvuje právo každého, jehož práva a svobody zaručené unijním právem byly porušeny, na účinné prostředky nápravy před soudem¹⁹⁰. Podle druhého pododstavce tohoto článku má každý právo, aby jeho věc byla projednána nezávislým a nestranným soudem¹⁹¹. Přístup k nezávislému soudu spadá do podstaty práva zaručeného v článku 47 Listiny¹⁹².

316. Toto právo na individuální soudní ochranu doplňuje povinnost členských států na základě článků 7 a 8 Listiny podrobit jakékoli sledování předchozímu přezkumu soudem nebo nezávislým správním orgánem, s výjimkou řádně odůvodněných naléhavých případů¹⁹³.

317. Jak tvrdily německá a francouzská vláda, právo na účinnou soudní ochranu zajisté nepředstavuje absolutní záruku¹⁹⁴, neboť toto právo může být omezeno z důvodů národní bezpečnosti. Odchytky jsou však povoleny pouze tehdy, pokud neporušují podstatu tohoto práva a jsou striktně nezbytné k dosažení oprávněného cíle.

318. V tomto ohledu Soudní dvůr v rozsudku Schrems rozhodl, že právní úprava, která nestanoví procesním subjektům *žádnou možnost* využít právních prostředků s cílem získat přístup k osobním údajům, které se jich týkají, nebo dosáhnout opravy či výmazu těchto údajů, nerespektuje podstatu základního práva zakotveného v článku 47 Listiny¹⁹⁵.

319. Zdůrazňuji, že toto právo na přístup implikuje oprávnění osoby získat od veřejných orgánů, s výhradou odchylek striktně nezbytných pro sledování oprávněného zájmu, *potvrzení skutečnosti, že zpracovávají či nezpracovávají osobní údaje, které se jí týkají*¹⁹⁶. To je podle mého názoru praktický dosah práva na přístup, pokud dotyčná osoba neví, zda veřejné orgány uchovaly osobní údaje, které se jí týkají, zejména po skončení procesu automatizovaného filtrování toků elektronických komunikací.

190 – Vysvětlení k Listině v tomto ohledu stanoví, že „v právu Unie je ochrana [stanovená v článku 47 Listiny] širší [než ochrana přiznaná článkem 13 EÚLP], neboť je zaručeno právo na účinnou soudní ochranu“. Viz rovněž stanovisko generálního advokáta M. Watheleta ve věci *Berlioz Investment Fund* (C-682/15, EU:C:2017:2, bod 37).

191 – Při posouzení postavení orgánu coby „soudu“ v rámci použití článku 47 Listiny musí být zohledněno to, zda je daný orgán zřízen zákonem, zda se jedná o stálý orgán, zda má obligatorní jurisdikci, zda má řízení před ním kontradiktorní povahu, zda aplikuje právní normy a zda je nezávislý. Viz rozsudek ze dne 27. února 2018, *Associação Sindical dos Juizes Portugueses* (C-64/16, EU:C:2018:117, bod 38 a citovaná judikatura).

192 – Viz zejména rozsudky ze dne 25. července 2018, *Minister for Justice and Equality (Nedostatky soudního systému)* (C-216/18 PPU, EU:C:2018:586, body 59 a 63); ze dne 5. listopadu 2019, *Komise v. Polsko (Nezávislost obecných soudů)* (C 192/18, EU:C:2019:924, bod 106), a ze dne 19. listopadu 2019, *A. K. a další (Nezávislost kárného kolegia Nejvyššího soudu)* (C-585/18, C-624/18 a C-625/18, EU:C:2019:982, bod 120).

193 – Viz bod 293 tohoto stanoviska. Článek 45 odst. 3 písm. a) GDPR stanoví, že při posuzování odpovídající úrovně ochrany poskytované třetím státem se zohlední existence „účinné správní a soudní ochrany“ pro subjekty údajů (kurzivou zvýraznil autor stanoviska). Stejně tak musí být podle bodu 104 odůvodnění GDPR přijetí rozhodnutí o odpovídající úrovni ochrany podřízeno podmínce, že subjektům údajů musí být poskytnuta „účinná správní a soudní ochrana“ (kurzivou zvýraznil autor stanoviska). Viz rovněž Skupina 29, EU-U. S. Privacy Shield – First Annual Joint Review, 28. listopadu 2017, WP 255 (bod B.3); usnesení Parlamentu ze dne 5. července 2018 o přiměřenosti ochrany poskytované štítem EU – USA na ochranu soukromí, P8_TA(2018)0315 (body 25 a 30), a EDPB, EU-U. S. Privacy Shield – Second Annual Joint Review, 22. ledna 2019 (body 94 až 97).

194 – V tomto smyslu viz rozsudek ze dne 28. února 2013, *Přezkum ve věci Arango Jaramillo a další v. EIB* (C-334/12 RX-II, EU:C:2013:134, bod 43).

195 – Rozsudek Schrems (bod 95).

196 – Článek 15 GDPR, nadepsaný „Právo subjektu údajů na přístup k osobním údajům“, stanoví v odstavci 1, že tento subjekt údajů „má právo získat od správce potvrzení, zda osobní údaje, které se ho týkají, jsou, či nejsou zpracovávány, a pokud je tomu tak, má právo získat přístup k těmto osobním údajům“. „Zásada přístupu“ stanovená v příloze II bodě II.8 písm. a) rozhodnutí o štítu na ochranu soukromí má stejný význam.

320. Kromě toho z judikatury vyplývá, že orgány členského státu jsou v zásadě povinny oznámit přístup k údajům, a *to od okamžiku, kdy tímto oznámením nebude možné ohrozit probíhající vyšetřování*¹⁹⁷. Takové oznámení totiž představuje nezbytný předpoklad pro výkon práva na nápravu na základě článku 47 Listiny¹⁹⁸. Tato povinnost je nyní převzata v čl. 23 odst. 2 písm. h) GDPR.

321. Body 111 až 135 rozhodnutí o štítu na ochranu soukromí uvádí stručně veškeré prostředky nápravy dostupné subjektům, jejichž údaje jsou předávány, pokud se obávají, že jejich údaje budou po předání zpracovány americkými zpravodajskými službami. Tyto prostředky nápravy byly rovněž popsány v rozsudku High Court (Vrchní soud) ze dne 3. října 2017, jakož i ve vyjádření zejména vlády Spojených států.

322. Není nutné podrobně připomínat znění těchto písemností. Předkládající soud totiž zpochybňuje odpovídající úroveň záruk týkajících se právní ochrany subjektů údajů primárně z důvodu, že obzvláště striktní požadavky týkající se aktivní legitimace (*standing*)¹⁹⁹ ve spojení s neexistencí jakékoli povinnosti oznamovat sledování osobám, které byly jeho předmětem, *i když by oznámení neohrozilo cíle*, v praxi nadměrně ztěžují výkon prostředků nápravy stanovených v právu Spojených států. Tyto pochybnosti sdílí DPC, M. Schrems, rakouská, polská a portugalská vláda, jakož i EDPB²⁰⁰.

323. V tomto ohledu se omezím na připomenutí, že pravidla v oblasti aktivní legitimace nemohou narušit účinnou soudní ochranu²⁰¹, jakož i na konstatování, že rozhodnutí o štítu na ochranu soukromí neuvádí žádný požadavek informovat subjekty údajů o tom, že byly předmětem sledovacích opatření²⁰². Jelikož neexistence povinnosti oznámit takové opatření, a to i v případech, kdy by oznámení subjektu údajů neškodilo účinnosti takového opatření, může bránit ve výkonu prostředků soudní nápravy, jeví se tato neexistence s ohledem na judikaturu uvedenou v bodě 320 tohoto stanoviska jako problematická.

324. Poznámka pod čarou 169 rozhodnutí o štítu na ochranu soukromí mimoto uznává, že dostupné právní kroky „závisí buď na existenci škody [...], nebo na prokázání toho, že vláda hodlá použít nebo zveřejnit informace získané [...] z elektronického sledování dotčené osoby proti této osobě“. Jak zdůraznil předkládající soud, DPC a M. Schrems, tento požadavek je v rozporu s judikaturou Soudního dvora, podle níž není k prokázání existence zásahu do základního práva na respektování soukromého života důležité, zda dotčené osoby utrpěly z důvodu tohoto zásahu případné nepříznivé následky²⁰³.

197 – Rozsudek Tele2 Sverige (bod 121), jakož i posudek 1/15 (bod 220). Jak poznamenala společnost Facebook Ireland, oznámení přístupu veřejných orgánů k údajům nemůže být vyžadováno systematicky. V tomto ohledu má ESLP za to, že „[n]ení možné v praxi požadovat oznámení a *posteriori*“, jelikož hrozba, která je předmětem sledování, „může trvat po dobu let či dokonce desetiletí“ po ukončení těchto opatření, takže oznámení může „narušovat dlouhodobý cíl, který odůvodňoval zahájení sledování“, jakož i „odhalovat metody práce zpravodajských služeb, jejich oblasti činnosti a [...] totožnost jejich agentů“ [rozsudek Zacharov (§ 287 a citovaná judikatura)]. V případě neexistence oznámení, ačkoli nelze tudíž uplatnit individuální prostředky nápravy v případě porušení zákonných požadavků, mohou další záruky stačit k ochraně práva na respektování soukromého života (viz rovněž rozsudek Centrum för Rättvisa, § 164 až 167 a 171 až 178). Viz bod 330 tohoto stanoviska.

198 – V tomto ohledu viz poznámka pod čarou 216 tohoto stanoviska.

199 – Viz bod 67 tohoto stanoviska.

200 – Viz EDPB, EU-U. S. Privacy Shield – Second Annual Joint Review, 22. ledna 2019 (s. 18, bod 97).

201 – Viz zejména rozsudky ze dne 11. července 1991, Verholen a další (C-87/90 až C-89/90, EU:C:1991:314, bod 24 a citovaná judikatura), jakož i ze dne 28. února 2013, Přezkum ve věci Arango Jaramillo a další v. EIB (C-334/12 RX-II, EU:C:2013:134, bod 43).

202 – Vláda Spojených států nicméně stejně jako předkládající soud upřesnila, že sledování na základě článku 702 FISA musí být oznámeno dotčené osobě, pokud jsou shromážděné údaje využity proti ní v rámci soudního řízení.

203 – Rozsudek ze dne 20. května 2003, Österreichischer Rundfunk a další (C-465/00, C-138/01 a C-139/01, EU:C:2003:294, bod 75); rozsudek Digital Rights Ireland (bod 33), rozsudek Schrems (bod 87) a posudek 1/15 (bod 124).

325. Kromě toho názor vyjádřený společností Facebook Ireland a vládou Spojených států, podle kterého jsou nedostatky charakterizující soudní ochranu subjektů, jejichž údaje jsou předávány do Spojených států, kompenzovány předběžnými kontrolami a kontrolami *a posteriori* vykonávanými Soudem pro uplatňování zákona FISA, jakož i četnými mechanismy dohledu vytvořenými v rámci výkonné a zákonodárné moci²⁰⁴, mne nepřesvědčuje.

326. Již jsem uvedl, že jednak v souladu se zjištěními uvedenými v rozhodnutí o štítu na ochranu soukromí nekontroluje Soud pro uplatňování zákona FISA jednotlivá sledovací opatření před jejich provedením²⁰⁵. Kromě toho, jak uvádí bod 109 odůvodnění tohoto rozhodnutí a jak potvrdila vláda Spojených států ve své písemné odpovědi na otázky Soudního dvora, je cílem kontroly použití selektorů prováděné *ex post* ověřit dodržení podmínek, jimiž se řídí výběr selektorů stanovených v ročním osvědčení, v případě, kdy zpravodajská agentura oznámí Soudu pro uplatňování zákona FISA incident týkající se možného porušení postupů zaměřených na zacílení a minimalizaci²⁰⁶. Řízení před Soudem pro uplatňování zákona FISA proto podle všeho neposkytuje individuální účinný prostředek nápravy osobám, jejichž údaje jsou předávány do Spojených států.

327. Třebaže mohou mimosoudní mechanismy kontroly uvedené v bodech 95 až 110 odůvodnění rozhodnutí o štítu na ochranu soukromí případně posílit jiné soudní prostředky nápravy, nemohou podle mého názoru postačovat k zajištění odpovídající úrovně ochrany s ohledem na právo subjektu údajů na nápravu. Konkrétně generální inspektoři, kteří patří do vnitřní struktury každé agentury, podle mého názoru nepředstavují nezávislé kontrolní mechanismy. Dohled vykonávaný PCLOB a zpravodajskými komisemi Kongresu se nerovná mechanismu individuální nápravy proti sledovacím opatřením.

328. Bude tedy třeba přezkoumat, zda úřad ombudsmana tyto mezery napravuje tím, že subjektům údajů poskytuje účinný prostředek nápravy před nezávislým a nestranným orgánem²⁰⁷.

329. Zadruhé připomínám, že pro účely posouzení opodstatněnosti zjištění o odpovídající úrovni ochrany provedeného v rozhodnutí o štítu na ochranu soukromí z hlediska prostředků nápravy dostupných osobám, které se domnívají, že byly předmětem sledování založeného na EO 12333, spočívá relevantní referenční rámec v ustanoveních EÚLP.

330. Jak bylo uvedeno výše²⁰⁸, ESLP provádí za účelem posouzení, zda sledovací opatření odpovídá podmínkám „předvídatelnosti“ a „nezbytnosti v demokratické společnosti“ ve smyslu čl. 8 odst. 2 EÚLP²⁰⁹, přezkum všech kontrolních a dozorových mechanismů prováděných „před, v průběhu a po“ jeho realizaci. Je-li v podání individuální žaloby bráněno tím, že oznámení sledovacího opatření není

204 – Tyto mechanismy jsou popsány v bodech 95 až 110 odůvodnění rozhodnutí o štítu na ochranu soukromí. Komise v nich v rámci kategorie pravidel týkajících se „účinné soudní ochrany“ odlišuje mechanismy dohledu (viz body 92 až 110 odůvodnění) od individuálních náprav (viz body 111 až 124 odůvodnění).

205 – Viz bod 298 tohoto stanoviska.

206 – Podle bodu 109 odůvodnění rozhodnutí o štítu na ochranu soukromí „[d]održování předpisů ověřují ministr spravedlnosti a ředitel [NSA], přičemž agentury mají povinnost hlásit veškeré případy nedodržení Soudu pro uplatňování zákona FISA [...], který na tomto základě může povolení změnit“.

207 – Viz body 333 až 340 tohoto stanoviska.

208 – Viz bod 305 tohoto stanoviska.

209 – V judikatuře týkající se sledování telekomunikací se ESLP zabýval otázkou prostředků nápravy v rámci přezkumu „postavení zákona“ a nezbytnosti zásahu do výkonu práva zaručeného článkem 8 EÚLP [viz zejména rozsudky Zacharov (§ 236) a Centrum för Rättvisa (§ 107)]. ESLP v rozsudku ze dne 1. července 2008, Liberty a další v. Spojené království (CE:ECHR:2008:0701JUD005824300, § 73), v rozsudku Zacharov (§ 307) a v rozsudku Centrum för Rättvisa (§ 184) poté, co konstatoval porušení článku 8 EÚLP, nepovažoval za nutné přezkoumat samostatně výtku vycházející z článku 13 této úmluvy.

možné, aniž by byla ohrožena jeho účinnost²¹⁰, může být tato mezera vyvážena prováděním nezávislé kontroly před použitím dotčeného opatření²¹¹. I když tedy ESLP považuje takové oznámení za „žádoucí“, pokud k němu může dojít bez narušení účinnosti sledovacího opatření, nezakotvil jej jako požadavek²¹².

331. V tomto ohledu z rozhodnutí o štítu na ochranu soukromí nevyplývá, že by sledovací opatření založená na EO 12333 byla oznamována dotčeným jednotlivcům nebo doprovázena mechanismy nezávislého soudního či správního přezkumu v jakékoli fázi jejich přijetí nebo jejich provádění.

332. Za těchto podmínek je třeba zkoumat, zda možnost obrátit se na ombudsmana nicméně umožňuje zajistit nezávislou kontrolu nad sledovacími opatřeními, a to i tehdy, jsou-li založena na EO 12333.

2) K dopadu mechanismu ombudsmana na úroveň ochrany práva na účinnou právní ochranu

333. Podle bodu 116 odůvodnění rozhodnutí o štítu na ochranu soukromí je cílem mechanismu ombudsmana popsaneho v příloze III A tohoto rozhodnutí poskytnout dodatečnou možnost nápravy, k níž by měli přístup všechny subjekty, jejichž údaje jsou předávány z Unie do Spojených států.

334. Jak zdůraznila vláda Spojených států, přípustnost stížnosti podané u ombudsmana není podmíněna dodržením pravidel v oblasti aktivní legitimace obdobných těm, které upravují přístup k americkým soudům. Bod 119 odůvodnění uvedeného rozhodnutí v tomto ohledu upřesňuje, že možnost obrátit se na ombudsmana nevyžaduje, aby subjekt údajů prokázal, že vláda Spojených států získala přístup k jeho osobním údajům.

335. Stejně jako DPC, M. Schrems, polská a portugalská vláda, jakož i EPIC, pochybují o schopnosti tohoto mechanismu kompenzovat nedostatky v soudní ochraně poskytované subjektům, jejichž údaje jsou předávány z Unie do Spojených států.

336. Především i když mechanismus mimosoudního přezkumu může představovat účinný prostředek nápravy ve smyslu článku 47 SFEU, je tomu tak zejména pouze tehdy, pokud je dotčený orgán zřízen zákonem a splňuje podmínku nezávislosti²¹³.

210 – I když podle ESLP neexistence oznámení v jakémkoli stadiu nebrání nutně tomu, aby sledovací opatření odpovídalo podmínce „nezbytnosti v demokratické společnosti“, narušuje přístup k soudům a tudíž efektivitu prostředků nápravy [viz zejména rozsudek ze dne 6. září 1978, Klass a další v. Německo (CE:ECHR:1978:0906JUD000502971, § 57 a 58); rozhodnutí Weber a Saravia (§ 135) a rozsudek Zacharov (§ 302)].

211 – V tomto smyslu viz rozsudek Centrüm för Rättvisa (§ 105).

212 – V rozsudku Big Brother Watch (§ 317) ESLP odmítl zařadit mezi minimální použitelné záruky sledovacího režimu založeného na rozsáhlém odposlouchávání elektronických komunikací požadavek oznámení sledování subjektům údajů. Viz rovněž rozsudek Centrüm för Rättvisa (§ 164). Přidělení těchto rozsudků velkému senátu ESLP má zejména za cíl přezkum tohoto závěru.

213 – Pojem „nezávislost“ zahrnuje první, vnější aspekt, který předpokládá, že je dotčený orgán chráněn před vnějšími zásahy nebo tlaky, které by mohly ohrozit nezávislost rozhodování jeho členů, pokud jde o spory, které jim jsou předloženy. Druhý, vnitřní aspekt souvisí s pojmem „nestrannost“ a týká se rovného odstupu ve vztahu ke stranám sporu a jejich příslušným zájmům s ohledem na předmět sporu. Viz zejména rozsudky ze dne 19. září 2006, Wilson (C-506/04, EU:C:2006:587, body 50 až 52); ze dne 25. července 2018, Minister for Justice and Equality (Nedostatky soudního systému) (C-216/18 PPU, EU:C:2018:586, body 63 a 65), a ze dne 19. listopadu 2019, A. K. a další (Nezávislost kárného kolegia Nejvyššího soudu) (C 585/18, C 624/18 a C 625/18, EU:C:2019:982, body 121 a 122). V souladu se zásadou dělby moci musí být nezávislost soudů zaručena zejména ve vztahu k moci výkonné. Viz rozsudek ze dne 19. listopadu 2019, A. K. a další (Nezávislost kárného kolegia Nejvyššího soudu) (C 585/18, C 624/18 a C 625/18, EU:C:2019:982, bod 127 a citovaná judikatura).

337. Z rozhodnutí o štítu na ochranu soukromí přitom vyplývá, že mechanismus ombudsmana, který vychází z PPD 28²¹⁴, není zřízen zákonem. Ombudsman je ustanoven ministrem zahraničních věcí a je nedílnou součástí ministerstva zahraničí Spojených států²¹⁵. Toto rozhodnutí neobsahuje žádný údaj o tom, že by odvolání ombudsmana nebo zrušení jeho jmenování bylo spojeno se zvláštními zárukami²¹⁶. I když je ombudsman prezentován jako nezávislý na „zpravodajské komunitě“, odpovídá ministru zahraničních věcí, a není tedy nezávislý na výkonné moci²¹⁷.

338. Dále účinnost mimosoudního prostředku nápravy závisí podle mého názoru rovněž na schopnosti dotčeného orgánu přijímat závazná a odůvodněná rozhodnutí. V tomto ohledu rozhodnutí o štítu na ochranu soukromí neobsahuje žádnou informaci o tom, že by ombudsman taková rozhodnutí přijímal. Nestanoví, že by úřad ombudsmana umožňoval žalobcům přístup k údajům, které se jich týkají, a jejich opravu nebo jejich výmaz, ani že by ombudsman přiznával osobám poškozeným sledovacím opatřeními nápravu. Konkrétně, jak vyplývá z přílohy III A bodu 4 písm. e) tohoto rozhodnutí, „ombudsman [...] nepotvrdí ani nevyvrátí, zda byla fyzická osoba cílem sledování, ani nepotvrdí konkrétní opravný prostředek, který byl použit“²¹⁸. Jestliže se americká vláda zavázala k tomu, aby jakékoli porušení příslušných norem odhalených ombudsmanem bylo napraveno dotčeným útvarům zpravodajských služeb²¹⁹, uvedené rozhodnutí neuvádí právní záruky, které by doprovázely tento závazek a kterých by se mohli dovolávat dotčení jednotlivci.

339. V důsledku toho úřad ombudsmana podle mého názoru neposkytuje prostředek nápravy u nezávislého orgánu, který by poskytoval subjektům, jejichž údaje jsou předávány, možnost uplatnit své právo na přístup k údajům nebo napadnout případná porušení příslušných pravidel ze strany zpravodajských služeb.

340. Konečně v souladu s judikaturou dodržování práva zaručeného v článku 47 Listiny předpokládá možnost následně podrobit rozhodnutí takového správního orgánu, který sám nesplňuje podmínku nezávislosti, kontrole ze strany soudu, který musí mít mimo jiné pravomoc rozhodovat o všech relevantních otázkách²²⁰. Podle informací poskytnutých v rozhodnutí o štítu na ochranu soukromí však nejsou rozhodnutí ombudsmana předmětem nezávislého soudního přezkumu.

341. Za těchto podmínek, jak tvrdili DPC, M. Schrems, EPIC, jakož i polská a portugalská vláda, je podstatná rovnocennost mezi soudní ochranou poskytovanou v právním řádu Spojených států osobám, jejichž údaje jsou do Spojených států předávány z Unie, a soudní ochranou, která vyplývá z GDPR vykládaného ve světle článku 47 Listiny a článku 8 EÚLP, sporná.

214 – Příloha III A rozhodnutí o štítu na ochranu soukromí odkazuje v tomto ohledu na oddíl 4 písm. d) PPD 28.

215 – Viz bod 116 odůvodnění rozhodnutí o štítu na ochranu soukromí.

216 – V rozsudku ze dne 31. května 2005, Syfait a další (C-53/03, EU:C:2005:333, bod 31), Soudní dvůr zdůraznil význam takových záruk pro splnění podmínky nezávislosti. V tomto ohledu viz rovněž rozsudky ze dne 24. června 2019, Komise v. Polsko (Nezávislost Nejvyššího soudu) (C-619/18, EU:C:2019:531, bod 76), a ze dne 5. listopadu 2019, Komise v. Polsko (Nezávislost obecných soudů) (C-192/18, EU:C:2019:924, bod 113).

217 – Viz body 65 a 121 odůvodnění, jakož i příloha III A bod 1 rozhodnutí o štítu na ochranu soukromí.

218 – Mimoto bod 121 odůvodnění rozhodnutí o štítu na ochranu soukromí stanoví, že „ombudsman bude muset ‚osvědčit‘, zda i) byla stížnost řádně prošetřena a zda ii) bylo dodrženo právo USA – včetně omezení a ochranných opatření uvedených v příloze VI – nebo v případě nedodržení bylo takové porušení napraveno“.

219 – Komise v rámci třetího výročního přezkumu štítu na ochranu soukromí konstatovala, že podle tvrzení vlády Spojených států v případě, že vyšetřování vedené ombudsmanem odhalí porušení postupů cíleného sběru a minimalizace povolených Soudem pro uplatňování zákona FISA, musí být toto porušení předloženo tomuto soudu. Soud pro uplatňování zákona FISA pak provede nezávislé vyšetřování a v případě potřeby uloží dotčené zpravodajské agentuře povinnost nápravy takového porušení. Viz Commission staff working document accompanying the report from the Commission to the European Parliament and the Council on the third annual review of the functioning of the EU-U. S. Privacy Shield, 23. října 2019, SWD(2019) 390 final, s. 28. Komise v něm odkazuje na dokument nadepsaný „Privacy Shield Ombudsperson Mechanism Unclassified Implementation Procedure“, dostupný na adrese <https://www.state.gov/wp-content/uploads/2018/12/Ombudsperson-Mechanism-Implementation-Procedures-UNCLASSIFIED.pdf> (s. 4 a 5).

220 – Viz rozsudky ze dne 16. května 2017, Berlioz Investment Fund (C-682/15, EU:C:2017:373, bod 55), a ze dne 13. prosince 2017, El Hassani (C-403/16, EU:C:2017:960, bod 39).

342. S přihlédnutím ke všem výše uvedeným úvahám mám určité pochybnosti ohledně souladu rozhodnutí o štítu na ochranu soukromí s čl. 45 odst. 1 GDPR vykládaného ve světle článků 7, 8 a 47 Listiny, jakož i článku 8 EÚLP.

V. Závěry

343. Navrhuji Soudnímu dvoru, aby odpověděl na předběžné otázky položené High Court (Vrchní soud, Irsko) následovně:

„Z analýzy předběžných otázek nevyplynulo nic, co by se mohlo dotknout platnosti rozhodnutí Komise 2010/87/EU ze dne 5. února 2010 o standardních smluvních doložkách pro předávání osobních údajů zpracovatelům usazeným ve třetích zemích podle směrnice Evropského parlamentu a Rady 95/46/ES, ve znění prováděcího rozhodnutí Komise (EU) 2016/2297 ze dne 16. prosince 2016.“