Sbírka soudních rozhodnutí

STANOVISKO GENERÁLNÍHO ADVOKÁTA
MACIEJE SZPUNARA
přednesené dne 28. září 2023 [1]

Věc C-470/21

La Quadrature du Net,
Fédération des fournisseurs d'accès à Internet associatifs,
Franciliens.net,
French Data Network
proti
Premier ministre,
Ministère de la Culture

[žádost o rozhodnutí o předběžné otázce, kterou podala Conseil d'État (Státní rada, Francie)]

„Řízení o předběžné otázce – Zpracování osobních údajů a ochrana soukromí v odvětví elektronických komunikací – Směrnice 2002/58/ES – Článek 15 odst. 1 – Pravomoc členských států omezit rozsah určitých práv a povinností – Povinnost předchozího přezkumu soudem nebo nezávislým správním orgánem s donucovací pravomocí – Údaje o totožnosti odpovídající IP adrese"

I. Úvod

1. Na žádost velkého senátu, předloženou na základě čl. 60 odst. 3 jednacího řádu Soudního dvora, rozhodl tento soud dne 7. března 2023 o přidělení projednávané věci plénu.

2. Usnesením ze dne 23. března 2023 rozhodl Soudní dvůr (plénum) o znovuotevření ústní části řízení a vyzval zúčastněné strany uvedené v článku 23 Statutu Soudního dvora Evropské unie, jakož i Evropského inspektora osobních údajů (EIOÚ) a Evropskou agenturu pro kybernetickou bezpečnost (ENISA), aby se zúčastnili nového jednání.

3. Dne 27. října 2022 jsem přednesl první stanovisko v této věci před ukončením ústní části řízení. Toto nové stanovisko je tedy pro mě příležitostí prohloubit určité aspekty mých úvah v této věci týkající se uchovávání osobních údajů a přístupu k nim.

[1] – Původní jazyk: francouzština.

II. Právní rámec

A. Unijní právo

4. V bodech 2, 6, 7, 11, 22, 26 a 30 odůvodnění směrnice 2002/58/ES [2] se uvádí:

„(2) tato směrnice usiluje o respektování základních práv a zachovává zásady uznané zejména v [Listině základních práv Evropské unie (dále jen ‚Listina')]. Tato směrnice zejména usiluje o to, aby byla plně dodržována práva stanovená v článcích 7 a 8 uvedené Listiny.

[…]

(6) internet převrací tradiční struktury trhu tím, že poskytuje společnou, obecnou infrastrukturu pro široký okruh služeb elektronických komunikací. Veřejně dostupné služby elektronických komunikací prostřednictvím internetu otevírají uživatelům nové možnosti, ale zároveň vytvářejí i nová rizika pro jejich osobní údaje a soukromí;

(7) v případě sítí veřejných komunikací je nutno přijmout zvláštní právní, regulační a technická ustanovení na ochranu základních práv a svobod fyzických osob a ochranu oprávněných zájmů právnických osob, zejména s ohledem na zvyšující se kapacitu automatického uchovávání a zpracování údajů týkajících se účastníků a uživatelů.

[…]

(11) tato směrnice, obdobně jako směrnice [95/46/CE [3]], se netýká ochrany základních práv a svobod ve vztahu k činnostem, které se neřídí právem Společenství. Proto tato směrnice nemění stávající rovnováhu mezi právem jednotlivce na soukromí a možností, aby členské státy přijaly opatření uvedená v čl. 15 odst. 1 této směrnice, která jsou nezbytná pro ochranu veřejné bezpečnosti, obrany, bezpečnosti státu (včetně hospodářské prosperity státu, pokud jsou tyto činnosti spojeny s otázkami bezpečnosti státu) a pro prosazování trestního práva. Tato směrnice se tedy nedotýká možnosti členských států provádět zákonné zachycování elektronických sdělení nebo přijímat jiná opatření, je-li to nezbytné pro některý z těchto účelů a je-li to v souladu s Evropskou úmluvou o ochraně lidských práv a základních svobod [podepsanou v Římě dne 4. listopadu 1950], jak je vykládána v rozhodnutích Evropského soudu pro lidská práva. Tato opatření musí být vhodná, plně přiměřená vzhledem k zamýšlenému účelu a nezbytná v demokratické společnosti a musí být předmětem odpovídajících záruk v souladu s Evropskou úmluvou o ochraně lidských práv a základních svobod;

[…]

[2] – 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), ve znění směrnice Evropského parlamentu a Rady ze dne 25. listopadu 2009 (Úř. věst. 2009, L 337, s. 11) (dále jen „směrnice 2002/58").

[3] – Směrnice Evropského parlamentu a Rady ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (Úř. věst. 1995, L 281, s. 31; Zvl. vyd. 13/15, s. 355).

(22) zákaz uchovávat sdělení a s nimi spojené provozní údaje jinými osobami než samotnými uživateli nebo bez jejich souhlasu neznamená zákaz jakéhokoli automatického, zprostředkovaného a přechodného uchovávání takových informací, pokud k němu dochází výlučně z důvodu provedení přenosu v síti elektronických komunikací a za předpokladu, že informace nejsou uchovávány po dobu delší než nezbytně nutnou pro účely přenosu a řízení provozu, a že po dobu tohoto uchovávání zůstane zajištěna důvěrnost. […]

[…]

(26) údaje o účastnících, které jsou zpracovávány v rámci sítí elektronických komunikací pro navázání spojení a přenos informací, obsahují informace o soukromém životě fyzických osob a dotýkají se práva na ochranu jejich korespondence nebo se dotýkají oprávněných zájmů právnických osob. Takové údaje je možno uchovávat pouze v rozsahu, který je nezbytný pro poskytování služby pro účely účtování a platby za propojení, a to po omezenou dobu. Jakékoli další zpracování takových údajů […] je přípustné pouze za předpokladu, že účastník s tímto souhlasil na základě přesných a úplných informací o druhu následného zamýšleného zpracování, které obdržel od poskytovatele veřejně dostupných služeb elektronických komunikací, spolu s informací o právu účastníka nedat takový souhlas nebo svůj souhlas k takovému zpracování vzít zpět. […]

[…]

(30) systémy pro zajišťování sítí a služeb elektronických komunikací musí být navrženy tak, aby omezily na nutné minimum množství nezbytných osobních údajů. […]“

5. Článek 2 této směrnice, nadepsaný „Definice“, stanoví:

„[…]

Použijí se rovněž tyto definice:

(a) ‚uživatelem‘ se rozumí jakákoli fyzická osoba používající veřejně dostupnou službu elektronické komunikace pro soukromé či obchodní účely, přičemž není nezbytně nutné, aby byla účastníkem této služby;

(b) ‚provozními údaji‘ se rozumějí jakékoli údaje zpracovávané pro účely přenosu sdělení sítí elektronických komunikací nebo pro jeho účtování;

(c) ‚lokalizačními údaji‘ se rozumějí jakékoli údaje zpracovávané v síti elektronických komunikací nebo službou elektronických komunikací, které určují zeměpisnou polohu koncového zařízení uživatele veřejně dostupné služby elektronických komunikací;

(d) ‚sdělením‘ se rozumí jakákoli informace, která se vyměňuje nebo přenáší mezi určitým počtem zúčastněných stran prostřednictvím veřejně dostupné služby elektronických komunikací; toto nezahrnuje informace přenášené jako součást vysílání pro veřejnost prostřednictvím sítě elektronických komunikací s výjimkou případů, kdy lze informace přiřadit k identifikovatelnému účastníku nebo uživateli, který tyto informace přijímá;

[…]“

6. Článek 3 uvedené směrnice, nadepsaný „Dotčené služby“, stanoví:

„Tato směrnice se vztahuje na zpracování osobních údajů ve spojení s poskytováním veřejně dostupných služeb elektronických komunikací ve veřejných komunikačních sítích ve Společenství, včetně veřejných komunikačních sítí podporujících zařízení pro shromažďování a identifikaci údajů.“

7. Článek 5 téže směrnice, nadepsaný „Důvěrný charakter sdělení“, stanoví:

„1. Členské státy zajistí prostřednictvím vnitrostátních právních předpisů důvěrný charakter sdělení přenášených pomocí veřejné komunikační sítě a veřejně dostupných služeb elektronických komunikací a s nimi souvisejících provozních údajů. Zejména zakáží příposlech, odposlech, uchovávání nebo jiné druhy zachycování či sledování sdělení a s nimi souvisejících provozních údajů osobami jinými než uživateli bez souhlasu dotčených uživatelů, pokud k takovému jednání nejsou zákonem oprávněny v souladu s čl. 15 odst. 1. Tento odstavec nebrání technickému uchovávání, které je nezbytné pro přenos sdělení, aniž by tím byla dotčena zásada důvěrnosti.

[…]

3. Členské státy zajistí, aby uchovávání informací nebo získávání přístupu k již uchovávaným informacím bylo v koncovém zařízení účastníka nebo uživatele povoleno pouze pod podmínkou, že dotčený účastník či uživatel poskytl svůj souhlas poté, co mu byly poskytnuty jasné a úplné informace v souladu se směrnicí [95/46], mimo jiné o účelu zpracování. To nebrání technickému ukládání nebo takovému přístupu, jehož jediným účelem je provedení přenosu sdělení prostřednictvím sítě elektronických komunikací, nebo je-li to nezbytně nutné k tomu, aby mohl poskytovatel služeb informační společnosti poskytovat služby, které si účastník nebo uživatel výslovně vyžádal.“

8. Článek 6 směrnice 2002/58, nadepsaný „Provozní údaje“, stanoví:

„1. Provozní údaje vztahující se k účastníkům a uživatelům zpracovávané a uchovávané provozovatelem veřejné komunikační sítě nebo poskytovatelem veřejně dostupné služby elektronických komunikací, musí být vymazány nebo anonymizovány, jakmile již nejsou potřebné pro přenos sdělení, aniž by tímto byly dotčeny odstavce 2, 3 a 5 tohoto článku a čl. 15 odst. 1.

2. Je možno zpracovávat provozní údaje nezbytné pro účely účtování a stanovení plateb za propojení. Takovéto zpracování je přípustné pouze do konce období, v němž lze právně napadnout účet či uplatňovat nárok na platbu.

[…]“

9. Článek 15 této směrnice, nadepsaný „Použití některých ustanovení směrnice [95/46]“, stanoví v prvním odstavci:

„Členské státy mohou přijmout legislativní opatření, kterými omezí rozsah práv a povinností uvedených v článku 5, článku 6, čl. 8 odst. 1, 2, 3 a 4 a článku 9 této směrnice, pokud toto omezení představuje v demokratické společnosti nezbytné, vhodné a přiměřené opatření pro zajištění národní bezpečnosti (tj. bezpečnosti státu), obrany, veřejné bezpečnosti a pro prevenci,

vyšetřování, odhalování a stíhání trestných činů nebo neoprávněného použití elektronického komunikačního systému, jak je uvedeno v čl. 13 odst. 1 směrnice [95/46]. Za tímto účelem mohou členské státy mimo jiné přijmout legislativní opatření umožňující uchovávání údajů po omezenou dobu na základě důvodů uvedených v tomto odstavci. Veškerá opatření uvedená v tomto odstavci musí být v souladu s obecnými zásadami práva [Unie], včetně zásad uvedených v čl. 6 odst. 1 a 2 [SEU].“

B. Francouzské právo

1. Le code de la propriété intellectuelle (zákon o duševním vlastnictví)

10. Článek L. 331-12 zákona o duševním vlastnictví, ve znění použitelném na spor v původním řízení (dále jen „CPI“), stanoví:

„Haute Autorité pour la diffusion des œuvres et la protection des droits sur Internet [Vysoký úřad pro šíření děl a ochranu práv na internetu, dále jen ‚Hadopi‘] je nezávislý orgán veřejné moci.“

11. Článek L. 331-13 CPI stanoví:

„[Hadopi] zajišťuje:

[…]

2. ochranu [děl a předmětů chráněných autorským právem nebo právy souvisejícími v sítích elektronických komunikací] před porušováním těchto práv v sítích elektronických komunikací používaných k poskytování internetových veřejných komunikačních služeb; […]“

12. Článek L. 331-15 tohoto zákona stanoví:

„[Hadopi] se skládá z Rady a Komise pro ochranu práv. […]

[…]

Členové Rady a Komise pro ochranu práv nejsou při výkonu svých pravomocí podřízeni žádnému orgánu.“

13. Článek L. 331-17 uvedeného zákona stanoví:

„Komise pro ochranu práv přijímá opatření stanovená v článku L. 331-25.“

14. Článek L. 331-21 téhož zákona stanoví:

„Pro účely výkonu pravomocí Komisí pro ochranu práv má [Hadopi] k dispozici úředníky, kteří složili přísahu a jsou zmocněni [jeho] předsedou za podmínek stanovených nařízením přijatým v návaznosti na stanovisko Státní rady. […]

Členové Komise pro ochranu práv a úředníci uvedení v prvním pododstavci přijímají podání zaslaná uvedené komisi za podmínek stanovených v článku L. 331-24. Provádí přezkum skutkových okolností.

Pro potřeby řízení mohou získat veškeré dokumenty, a to na jakémkoli nosiči, včetně údajů uchovávaných a zpracovávaných provozovateli elektronických komunikací na základě článku L. 34-1 code des postes et des communications électroniques (zákon o poštovních službách a elektronických komunikacích) a poskytovateli uvedenými v čl. 6 odst. I bodech 1 a 2 loi n° 2004 575 du 21 juin 2004 pour la confiance dans l'économie numérique (zákon č. 2004-575 ze dne 21. června 2004 o podpoře důvěry v digitální ekonomiku).

Mohou rovněž obdržet kopii dokumentů uvedených v předchozím pododstavci.

Zejména mohou od provozovatelů elektronických komunikací získat totožnost, poštovní adresu, e-mailovou adresu a telefonní kontaktní údaje účastníka, jehož přístup k veřejným komunikačním službám on-line byl použit pro účely rozmnožování, zobrazování, zpřístupňování nebo sdělování chráněných děl nebo předmětů veřejnosti bez souhlasu nositelů práv […], pokud je takový souhlas vyžadován."

15. Článek L. 331-24 CPI stanoví:

„Komise pro ochranu práv jedná na základě podnětu pověřených úředníků […], které jmenují:

– řádně ustavené ochranné profesní organizace,

– kolektivní správci,

– Státní středisko filmové a animované tvorby.

Komise pro ochranu práv může jednat také na základě informací, které jí předá státní zástupce.

Komise se nemůže zabývat skutečnostmi, které nastaly před více než šesti měsíci."

16. Článek L. 331-25 tohoto zákona, upravující postup „odstupňované reakce", stanoví:

„Pokud byly Komisi pro ochranu práv předloženy skutečnosti, které mohou představovat nesplnění povinnosti stanovené v článku L. 336-3 [CPI], může účastníkovi […] zaslat doporučení, v němž mu připomene ustanovení článku L. 336-3, vyzve jej, aby splnil povinnost stanovenou v tomto článku, a upozorní jej na sankce, které mu hrozí podle článků L. 335-7 a L. 335-7-1. Toto doporučení rovněž obsahuje informace pro účastníka o legální nabídce internetového kulturního obsahu, o existenci bezpečnostních opatření, která mají zabránit porušování povinnosti stanovené v článku L. 336-3, jakož i o nebezpečí, které praktiky porušující autorská práva a práva s nimi související představují pro rozvoj umělecké tvorby a pro správu kulturního odvětví.

Pokud do šesti měsíců od vydání doporučení uvedeného v prvním odstavci dojde opětovně ke skutečnostem, které by mohly představovat nesplnění povinnosti stanovené v článku L. 336-3, může Komise zaslat nové doporučení obsahující stejné informace jako předchozí doporučení elektronickými prostředky […] K tomuto doporučení je Komise povinna připojit dopis předaný proti podpisu nebo jakýmkoli jiným způsobem umožňujícím prokázat datum doručení tohoto doporučení.

V doporučeních vydaných podle tohoto článku se uvede datum a čas, kdy byly zjištěny skutečnosti, které mohou představovat nesplnění povinnosti stanovené v článku L. 336-3. Nezveřejní se v nich však obsah chráněných děl nebo předmětů, kterých se toto nesplnění povinnosti týká.

V doporučení se uvedou telefonní čísla a poštovní a elektronická adresa, kam může adresát případně sdělit Komisi pro ochranu práv své připomínky, a pokud o to výslovně požádá, zjistit podrobnosti o obsahu chráněných děl nebo předmětů, jichž se údajné porušení týká.“

17. Článek L. 331-29 uvedeného zákona stanoví:

„[Hadopi] je oprávněn zavést automatizované zpracovávání osobních údajů osob, proti kterým je vedeno řízení podle tohoto pododdílu.

Účelem tohoto zpracování je provedení opatření stanovených v tomto pododdíle, všech souvisejících procesních úkonů a postupů za účelem informování ochranných profesních organizací a kolektivních správců o případném postoupení věci soudnímu orgánu, jakož i oznámení stanovených v pátém pododstavci článku L. 335-7, ze strany Komise pro ochranu práv.

Prováděcí předpisy k tomuto článku stanoví nařízení vlády […]. Nařízení vlády stanoví zejména:

– kategorie zaznamenávaných údajů a dobu jejich uchovávání,

– příjemce, kteří jsou oprávněni tyto údaje obdržet, zejména osoby, jejichž předmětem činnosti je poskytování přístupu k internetovým veřejným komunikačním službám;

– podmínky, za nichž mohou dotyčné osoby uplatnit u [Hadopi] své právo na přístup k údajům, které se jich týkají […]“

18. Článek R. 331-37 téhož zákona stanoví:

„Provozovatelé elektronických komunikací […] a poskytovatelé […] jsou povinni sdělit osobní údaje a informace uvedené v bodě 2 přílohy [décret nº 2010-236 du 5 mars 2010 relatif au traitement automatisé de données à caractère personnel autorisé par l'article L. 331-29 [CPI] dénommé ‚Système de gestion des mesures pour la protection des œuvres sur internet‘ (nařízení č. 2010-236 ze dne 5. března 2010, o automatizovaném zpracování osobních údajů povoleném článkem L. 331-29 [CPI] s názvem ‚Systém pro správu opatření na ochranu děl na internetu‘[4] (dále jen ‚nařízení ze dne 5. března 2010‘)] prostřednictvím propojení s automatizovaným zpracováním osobních údajů uvedeným v článku L. 331-29 nebo prostřednictvím záznamového média, které zajišťuje jejich integritu a bezpečnost, a to […] do osmi dnů od okamžiku, kdy jim Komise pro ochranu práv předá technické údaje nezbytné k identifikaci účastníka, jehož přístup k internetovým veřejným komunikačním službám byl použit pro účely rozmnožování, zobrazování, zpřístupňování nebo sdělování chráněných děl nebo předmětů veřejnosti bez souhlasu nositelů práv […], pokud je takový souhlas vyžadován.

[…]“

[4] – JORF ze dne 7. března 2010, text č. 19.

19. Článek R. 335-5 CPI stanoví:

„I.- Níže uvedená jednání držitele přístupu k internetovým veřejným komunikačním službám bez oprávněného důvodu jsou považována za hrubou nedbalost, za niž lze uložit pokutu stanovenou pro přestupky páté třídy, pokud jsou splněny podmínky stanovené v odstavci II:

1. nezavedení prostředku pro zabezpečení tohoto přístupu, nebo

2. nepostupování s náležitou péčí při zavedení takového prostředku.

II.- Ustanovení odstavce I se použijí pouze v případě, že jsou splněny tyto dvě podmínky:

1. držiteli přístupu bylo na základě článku L. 331-25 a způsobem v něm stanoveným Komisí pro ochranu práv doporučeno, aby zavedl prostředek k zabezpečení svého přístupu, který zabrání jeho opětovnému použití pro účely rozmnožování, zobrazování nebo zpřístupňování či sdělování veřejnosti děl nebo předmětů chráněných autorským právem nebo právem s ním souvisejícím bez souhlasu nositelů práv […], pokud je takový souhlas vyžadován,

2. do jednoho roku od doručení tohoto doporučení došlo k opětovnému použití tohoto přístupu k účelům uvedeným v pododstavci 1. tohoto odstavce II.“

20. Článek L. 336-3 tohoto zákona stanoví:

„Držitel přístupu k internetovým veřejným komunikačním službám je povinen zajistit, aby tento přístup nebyl používán pro účely rozmnožování, zobrazování, zpřístupňování nebo sdělování veřejnosti děl nebo předmětů chráněných autorským právem nebo právem s ním souvisejícím bez souhlasu nositelů […], pokud je takový souhlas vyžadován.

Nesplnění povinnosti stanovené v prvním odstavci ze strany držitele přístupu nezakládá trestní odpovědnost dotyčné osoby […]“

2. Nařízení vlády ze dne 5. března 2010

21. Článek 1 nařízení vlády ze dne 5. března 2010, ve znění použitelném na skutkové okolnosti sporu v původním řízení, stanoví:

„Účelem zpracování osobních údajů s názvem ‚Systém pro správu opatření na ochranu děl na internetu‘ je provádění následujících opatření ze strany Komise pro ochranu práv úřadu [Hadopi]:

1. opatření stanovená v knize III legislativní části zákona [CPI] (hlava III kapitola I oddíl 3 pododdíl 3) a v knize III prováděcí části téhož zákona (hlava III kapitola I oddíl 2 pododdíl 2),

2. podávání podnětů státnímu zástupci ohledně skutečností, které mohou představovat trestné činy stanovené v článcích L. 335-2, L. 335-3, L. 335-4 a R. 335-5 téhož zákona, jakož i informování ochranných profesních organizací a kolektivních správců o těchto podnětech,

[…]“

22. Článek 4 tohoto nařízení stanoví:

„I.- Jmenovaní úředníci pověření předsedou úřadu [Hadopi] podle článku L. 331-21 [CPI] a členové Komise pro ochranu práv uvedené v článku 1 mají přímý přístup k osobním údajům a informacím uvedeným v příloze tohoto nařízení.

II.- Provozovatelé elektronických komunikací a poskytovatelé služeb uvedení v bodě 2 přílohy tohoto nařízení obdrží:

– technické údaje potřebné k identifikaci účastníka,

– doporučení stanovená v článku L. 331-25 [CPI] za účelem jejich zaslání svým účastníkům elektronickými prostředky,

– informace nezbytné pro výkon vedlejších trestů pozastavení přístupu k internetové veřejné komunikační službě, o nichž státní zástupce uvědomil Komisi pro ochranu práv.

III.- Ochranné profesní organizace a kolektivní správci obdrží informace týkající se podnětu podaného ke státnímu zástupci.

IV.- Soudní orgány obdrží protokol o zjištění skutků, které by mohly představovat trestné činy stanovené v článcích L. 335-2, L. 335-3, L. 335-4, L. 335-7, R. 331-37, R. 331-38 a R. 335-5 [CPI].

O výkonu trestu pozastavení přístupu je informován automatizovaný rejstřík trestů.“

23. Příloha k nařízení vlády ze dne 5. března 2010 stanoví:

„Při zpracování údajů prostřednictvím ‚Systému pro správu opatření na ochranu děl na internetu‘ se zaznamenávají následující osobní údaje a informace:

1. osobní údaje a informace získané od řádně ustavených ochranných profesních organizací, kolektivních správců, Státního střediska filmové a animované tvorby a státního zástupce:

Pokud jde o jednání, které může představovat nesplnění povinnosti stanovené v článku L. 336-3 [CPI]:

datum a čas, kdy k jednání došlo,

IP adresa dotčených účastníků,

použitý protokol peer-to-peer,

pseudonym používaný účastníkem,

informace o chráněných dílech nebo předmětech, kterých se skutečnosti týkají,

název souboru uloženého v počítači účastníka (pokud existuje),

poskytovatel internetových služeb, u kterého byl přístup sjednán nebo který poskytl technický zdroj IP.

[…]

2. Osobní údaje a informace týkající se účastníka shromážděné od provozovatelů elektronických komunikací […] a poskytovatelů služeb […]:

příjmení, jména,

poštovní adresa a e-mailové adresy,

telefonní číslo,

adresa telefonního zařízení účastníka,

poskytovatel přístupu k internetu, který využívá technické prostředky poskytovatele internetových služeb uvedeného v bodě 1, s nímž účastník uzavřel smlouvu; číslo smlouvy,

datum začátku pozastavení přístupu k internetové veřejné komunikační službě.

[…]“

3. Le code des postes et des télécommunications (zákon o poštovních službách a elektronických komunikacích)

24. Článek L. 34-1 zákona o poštovních službách a elektronických komunikacích, ve znění článku 17 zákona č. 2021-998 ze dne 30. července 2021 [5], v odstavci IIa stanoví:

„[P]rovozovatelé elektronických komunikací jsou povinni uchovávat:

1. pro účely trestního řízení, předcházení ohrožení veřejné bezpečnosti a zajištění bezpečnosti státu údaje o totožnosti uživatele, a to po dobu pěti let od skončení platnosti jeho smlouvy,

2. pro stejné účely, jaké jsou uvedeny v pododstavci 1 tohoto odstavce IIa, další informace poskytnuté uživatelem při přihlášení ke smlouvě nebo vytvoření účtu, jakož i informace týkající se plateb, a to po dobu jednoho roku od skončení platnosti jeho smlouvy nebo zrušení jeho účtu;

3. za účelem boje proti závažné trestné činnosti a organizovanému zločinu, předcházení závažnému ohrožení veřejné bezpečnosti a ochrany národní bezpečnosti, technické údaje umožňující identifikaci zdroje připojení nebo údaje týkající se použitého koncového zařízení, a to po dobu jednoho roku od připojení nebo použití koncového zařízení.“

[5] – JORF ze dne 31. července 2021, text č. 1. Toto znění článku L. 34-1 tohoto zákona, platné od 31. července 2021, bylo přijato v návaznosti na rozhodnutí Conseil d'État (Státní rada, Francie) ze dne 21. dubna 2021, č. 393099 (JORF ze dne 25. dubna 2021), kterým bylo zrušeno předchozí znění tohoto ustanovení, jež zahrnovalo povinnost uchovávat osobní údaje „pro účely vyšetřování, zjišťování a stíhání trestných činů nebo nesplnění povinnosti definované v článku L. 336-3 [CPI]“, a to výhradně za účelem jejich případného poskytnutí mimo jiné úřadu Hadopi. V rozhodnutí č. 2021-976-977 QPC ze dne 25. února 2022 (p. Habib A. a další) Conseil constitutionnel (Ústavní rada, Francie) prohlásila toto předchozí znění článku L. 34-1 uvedeného zákona za protiústavní, a to zejména z důvodu, že „tím, že napadená ustanovení povolují obecné a nediferencované uchovávání údajů o připojení, porušují v nepřiměřené míře právo na respektování soukromého života“ (bod 13). Tento soud totiž dospěl k závěru, že údaje o připojení, které musí být podle těchto ustanovení uchovávány, se týkají nejen identifikace uživatelů služeb elektronických komunikací, ale zahrnují i další údaje, které „vzhledem ke své povaze, rozmanitosti a možným způsobům jejich zpracování […] poskytují rozsáhlé a přesné informace o těchto uživatelích a případně o třetích osobách, což představuje významný zásah do jejich soukromého života“ (bod 11).

III. Řízení před Soudním dvorem

25. Na výzvu určenou zúčastněným stranám uvedeným v článku 23 Statutu Soudního dvora Evropské unie odpověděli žalobci v původním řízení, francouzská, dánská, estonská, irská, nizozemská, finská a švédská vláda, jakož i Evropská komise na písemné otázky položené Soudním dvorem.

26. Tytéž strany, s výjimkou finské vlády, česká, španělská, kyperská, lotyšská a norská vláda, jakož i EIOÚ a ENISA, se zúčastnily jednání, které se konalo dne 15. května 2023.

IV. Analýza

27. Na základě analýzy předběžných otázek v mém prvním stanovisku jsem Soudnímu dvoru navrhl, aby rozhodl, že čl. 15 odst. 1 směrnice 2002/58 musí být vykládán v tom smyslu, že nebrání vnitrostátní právní úpravě, která umožňuje poskytovatelům služeb elektronických komunikací uchovávání a takovému správnímu orgánu, jako je Hadopi [6] přístup omezený na údaje o totožnosti odpovídající IP adresám, aby tento orgán mohl identifikovat držitele těchto IP adres, kteří jsou podezřelí z porušování práva autorského a práv s ním souvisejících, a případně vůči nim mohl přijmout odpovídající opatření, aniž tento přístup podléhá předchozímu přezkumu ze strany soudu nebo nezávislého správního orgánu, jsou-li tyto údaje jediným prostředkem vyšetřování umožňujícím identifikovat osobu, které byla tato adresa přidělena v okamžiku spáchání trestného činu.

28. V tomto stanovisku rozvedu podrobněji některé prvky mé předchozí analýzy a body diskutované na jednání konaném dne 15. května 2023 a uvedu důvody, proč trvám jak na svém návrhu odpovědi na předběžné otázky, tak na úvahách, které k němu vedly [7].

29. Konkrétně doložím, že povolení uchovávat údaje o totožnosti odpovídající IP adresám a přístup k nim bez předchozí kontroly za účelem identifikace pachatelů porušování, pokud tyto údaje představují jediný prostředek jejich identifikace, splňuje požadavky stanovené Soudním dvorem v souvislosti s přezkumem opatření přijatých podle čl. 15 odst. 1 směrnice 2002/58 (část B).

30. Zdůrazním přitom, že takové řešení nepředstavuje obrat v přísné judikatuře chránící základní práva, kterou Soudní dvůr vytvořil počínaje rozsudky Tele2 Sverige a Watson a další [8] a La Quadrature du Net a další [9], ale nezbytný vývoj této judikatury, který je podle mého názoru v souladu se zásadami stanovenými Soudním dvorem. Toto rozlišení není pouze sémantické. Řešení, které navrhuji, totiž nemá za cíl zpochybnit stávající judikaturu, ale v zájmu určitého pragmatismu umožnit její přizpůsobení za specifických a velmi úzce vymezených okolností (část C).

6 – Dne 1. ledna 2022 se z Conseil supérieur de l'audiovisuel (Nejvyšší rada pro audiovizuální vysílání, CSA) a Hadopi stala Autorité de régulation de la communication audiovisuelle et numérique (Úřad pro regulaci audiovizuální a digitální komunikace, Arcom). Vzhledem k období, v němž se odehrávaly skutečnosti ve sporu v původním řízení, však v tomto stanovisku budu odkazovat na Hadopi.

7 – V tomto ohledu rovněž trvám na svém návrhu přeformulovat předběžné otázky a na svém chápání jejich předmětu. Ačkoli se totiž znění otázek týká pouze přístupu k údajům o totožnosti odpovídajícím IP adresám, otázka přístupu k těmto údajům je neoddělitelná od otázky jejich uchovávání poskytovateli služeb elektronických komunikací, takže analýza slučitelnosti uchovávání s unijním právem je nezbytným předpokladem pro analýzu slučitelnosti přístupu. V tomto ohledu viz body 45 a násl. mého prvního stanoviska. Stejně tak, i když se předběžné otázky týkají „údajů o totožnosti odpovídající IP adrese“, je třeba je chápat jako otázky, které se týkají i přístupu k IP adresám, které umožňují identifikovat zdroj připojení. V tomto ohledu viz body 41 a násl. mého prvního stanoviska.

8 – Rozsudek ze dne 21. prosince 2016 (C-203/15 a C-698/15, dále jen „rozsudek Tele2“, EU:C:2016:970).

9 – Rozsudek ze dne 6. října 2020 (C-511/18, C-512/18 a C-520/18, dále jen „rozsudek La Quadrature du Net a další“, EU:C:2020:791).

31. Ve snaze o jasnost a vzhledem k tomu, že diskuse na jednání prokázaly v tomto ohledu potřebu upřesnění, připomenu na úvod své analýzy, jak funguje mechanismus odstupňované reakce, který provádí Hadopi (část A).

A. Mechanismus odstupňované reakce prováděný Hadopi

32. Hadopi je nezávislý správní orgán odpovědný za ochranu autorských práv a práv s nimi souvisejících proti porušování těchto práv na internetu. Za tímto účelem byl zaveden mechanismus tzv. odstupňované reakce, jehož prováděním je pověřena komise pro ochranu práv Hadopi.

33. Na tuto komisi se obracejí organizace zastupující nositele práv, v jejichž rámci určití přísežní zástupci schválení ministrem kultury shromažďují IP adresy uživatelů internetu na *peer-to-peer* sítích, kteří zpřístupňují díla veřejnosti bez svolení jejich majitelů. Poté jsou vypracovány protokoly. Obsahují zejména IP adresu internetového přístupu, který byl použit k porušení autorských práv, datum a čas zjištěného porušení a název daného díla a jsou předány komisi pro ochranu práv Hadopi. V této souvislosti je třeba zdůraznit, jak uvedl EIOÚ, že zpracování osobních údajů zástupci organizací zastupujících nositele práv podléhá povolení ze strany Commission nationale de l'informatique et des libertés (Národní komise pro informatiku a svobody, CNIL), která je francouzským orgánem dozoru nad ochranou údajů [10].

34. Po obdržení protokolů a automatické kontrole, zda obsahují všechny požadované údaje, může komise pro ochranu práv Hadopi získat od poskytovatelů služeb elektronických komunikací totožnost, poštovní adresu, e-mailovou adresu a kontaktní informace na majitele předplatného, které bylo použito k porušení autorského práva.

35. Hadopi pak může této osobě zaslat „doporučení", v němž ji informuje o tom, že její přístup k internetu byl použit způsobem porušujícím autorská práva, a uloží podezřelé osobě, která nesplnila svou povinnost obezřetnosti ohledně respektování děl chráněných autorským právem nebo právem s ním souvisejícím na internetu, aby toto doporučení splnila. Jinými slovy, doporučení je určeno držiteli přístupu k internetu, kterým může být ve skutečnosti někdo jiný než osoba, která dílo zpřístupnila v rozporu s autorským právem. Druhé doporučení může být vydáno v případě druhého zjištění porušení při použití stejného internetového přístupu. V případě opakovaného porušení práv může komise pro ochranu práv Hadopi rozhodnout o předložení věci státnímu zástupci k trestnímu stíhání. V tomto ohledu, jak francouzská vláda upřesnila ve svém prvním vyjádření, jsou zástupci Hadopi odpovědní za mechanismus odstupňované reakce přísežnými zástupci, oprávněnými předsedou Hadopi, jsou vázáni služebním tajemstvím a jako jediní v rámci Hadopi jsou oprávněni k přístupu k osobním údajům zpracovávaným v rámci tohoto mechanismu.

36. V této souvislosti je třeba upřesnit, že údaje, které jsou shromažďovány a předávány Hadopi, nejsou údaje všech uživatelů *peer-to-peer* sítí, pokud si tito uživatelé pouze stahují takový obsah [11], ale pouze údaje osob, které takový porušující obsah zpřístupnily, tj. které takový obsah *nahrály*.

[10] – V tomto ohledu viz rozhodnutí CNIL č. 2010-225 ze dne 10. června 2010, kterým se mění povolení pro Société des auteurs compositeurs et éditeurs de musique (SACEM) k provádění zpracování osobních údajů za účelem vyšetřování a zaznamenávání trestných činů padělání spáchaných prostřednictvím sítí pro výměnu souborů označovaných jako „peer to peer" (povolení č. 1425421).

[11] – Stran fungování *peer-to-peer* sítí a různých profilů internetových uživatelů na těchto sítích, viz mé stanovisko ve věci M. I. C. M. (C-597/19, EU:C:2020:1063, body 37 a násl.).

37. Pro ilustraci uvádím, že v roce 2021 Hadopi obdržel téměř čtyři miliony protokolů od organizací zastupující nositele práv, vydal 210 595 prvních doporučení a 53 564 druhých doporučení a předal 1 484 případů státnímu zástupci.

38. Po těchto připomenutích doložím, v čem takový mechanismus, který předpokládá uchovávání údajů o totožnosti odpovídajících IP adresám a přístup k nim, splňuje podle mého názoru požadavky judikatury týkající se vnitrostátních opatření přijatých podle čl. 15 odst. 1 směrnice 2002/58.

B. Dodržení požadavků judikatury Soudního dvora týkající se výkladu čl. 15 odst. 1 směrnice 2002/58

39. Vzhledem k tomu, že jsem již ve svém prvním stanovisku připomněl judikaturu Soudního dvora týkající se uchovávání IP adres přidělených zdroji připojení a přístupu k nim [12], zaměřím se v tomto stanovisku na to, co podle mého názoru tvoří jádro této judikatury, a to zaprvé požadavek přiměřenosti a zadruhé, pokud jde o přístup k těmto údajům, případnou nutnost předchozího přezkumu soudem nebo nezávislým správním orgánem.

1. K přiměřenosti dotčeného opatření

40. K tomu, aby bylo možné určit, zda je opatření týkající se uchovávání nebo přístupu k údajům o totožnosti odpovídajícím IP adrese slučitelné s unijním právem, je třeba, jak Soudní dvůr opakovaně zdůrazňuje, sladit jednotlivé oprávněné zájmy a dotčená práva, kterými jsou na jedné straně právo na respektování soukromí a na ochranu osobních údajů [13] zaručené články 7 a 8 Listiny, a na straně druhé ochrana práv a svobod druhých a práv zakotvených v článcích 3, 4, 6 a 7 Listiny [14]. Dodávám, že v projednávané věci je třeba sladit práva na ochranu soukromí a ochranu osobních údajů s právem na vlastnictví zakotveným v článku 17 Listiny, neboť mechanismus odstupňované reakce má v konečném důsledku za cíl chránit autorská práva a práva s nimi související.

41. Soudní dvůr v této souvislosti upřesňuje, že toto sladění, které se provádí podle čl. 15 odst. 1 směrnice 2002/58, umožňuje členským státům přijmout opatření, které se odchyluje od zásady důvěrnosti, pokud je takové opatření „v demokratické společnosti *nezbytné, přiměřené a úměrné*“ (kurzivou zvýraznil autor stanoviska). V bodě 11 odůvodnění této směrnice je upřesněno, že opatření této povahy musí být „plně“ *přiměřené* vzhledem k zamýšlenému účelu [15].

42. Soudní dvůr se krom toho na zásadu proporcionality odvolává ve všech svých úvahách týkajících se výkladu čl. 15 odst. 1 směrnice 2002/58, a činí ji tak základem přezkumu vnitrostátního opatření o uchovávání osobních údajů nebo přístupu k nim přijatého podle tohoto ustanovení.

[12] – Body 53 a násl. mého prvního stanoviska.

[13] – V kontextu směrnice 2002/58 se právo na respektování soukromí a na ochranu osobních údajů odráží v zásadách důvěrnosti sdělení a zákazu uchovávání s nimi souvisejících údajů, které tato směrnice stanoví.

[14] – Rozsudky La Quadrature du Net a další (body 120 až 122, jakož i 127 a 128); ze dne 5. dubna 2022, Commissioner of An Garda Síochána a další (C-140/20, dále jen „rozsudek Commissioner of An Garda Síochána a další“, EU:C:2022:258, body 48 a 50), jakož i ze dne 20. září 2022, SpaceNet a Telekom Deutschland (C-793/19 a C-794/19, dále jen „rozsudek SpaceNet a Telekom Deutschland“, EU:C:2022:702, body 63 a 65).

[15] – Rozsudky La Quadrature du Net a další (bod 129), Commissioner of An Garda Síochána a další (bod 51) a SpaceNet a Telekom Deutschland (bod 66).

43. Důkladnější výklad těchto úvah ukazuje, že zásada proporcionality má v kontextu čl. 15 odst. 1 směrnice 2002/58 různé aspekty týkající se jednak závažnosti zásahu do základních práv, který je spojen s uchováváním provozních údajů nebo přístupem k nim, a jednak nezbytnosti dotčeného opatření.

44. Pokud jde o uchovávání a přístup Hadopi k údajům o totožnosti odpovídajícím IP adresám, domnívám se, že jak závažnost zásahu, tak i nezbytnost těchto údajů by měly vést Soudní dvůr k tomu, aby přizpůsobil svůj přezkum přiměřenosti vnitrostátního opatření přijatého na základě čl. 15 odst. 1 směrnice 2002/58.

a) Závažnost zásahu do základních práv

45. Z ustálené judikatury Soudního dvora jasně vyplývá, že v souladu se zásadou proporcionality musí být význam cíle sledovaného opatřením přijatým na základě čl. 15 odst. 1 směrnice 2002/58 úměrný závažnosti zásahu, který z něj vyplývá [16].

46. Konkrétně Soudní dvůr rozhodl, jak jsem zdůraznil v mém prvním stanovisku, že v oblasti prevence, vyšetřování, odhalování a stíhání trestných činů může být odůvodněn závažný zásah pouze cílem spočívajícím v boji proti trestné činnosti, která musí být rovněž kvalifikována jako závažná [17].

47. Pokud jde o IP adresy, Soudní dvůr uvádí, že i když jsou méně citlivé než ostatní provozní údaje, jejich uchovávání a analýza přesto představují závažné zásahy do základních práv, jelikož mohou být použity k úplnému sledování postupu prohlížení uživatelem internetu, a vytvořit tak jeho podrobný profil a vyvodit přesné závěry o jeho soukromém životě [18].

48. Ve věci v původním řízení je účelem uchovávání údajů o totožnosti odpovídajícím IP adresám a přístupu k nim boj proti porušování autorského práva a práv s ním souvisejících. Podle mého názoru je přitom zřejmé, že tento boj nemůže spadat do oblasti boje proti závažné trestné činnosti [19], a to i pokud by byl objem takových porušení masivní. Existoval by tedy rozpor mezi závažností zásahu do základních práv, který s sebou nese dotčené opatření, a cílem, který tento zásah sleduje.

49. V mém prvním stanovisku jsem v souladu s judikaturou Soudního dvora zastával názor, že přístup Hadopi k údajům o totožnosti odpovídajícím IP adrese skutečně představuje závažný zásah do základních práv. I když jsem se rovněž domníval, že uchovávání těchto údajů a přístup k nim by měly být v projednávané věci přesto povoleny, musím v návaznosti na jednání učinit několik upřesnění.

16 – Rozsudky Commissioner of An Garda Síochána a další (bod 56) a SpaceNet a Telekom Deutschland (bod 71).

17 – Rozsudky Tele2 (bod 115); ze dne 2. října 2018, Ministerio Fiscal (C-207/16, EU:C:2018:788, bod 56), a ze dne 2. března 2021, Prokuratuur (Podmínky přístupu k údajům týkajícím se elektronických komunikací) (C-746/18, dále jen „rozsudek Prokuratuur“, EU:C:2021:152, bod 33). Rovněž viz bod 92 mého prvního stanoviska.

18 – Viz rozsudky La Quadrature du Net a další (body 152 a 153); Commissioner of An Garda Síochána a další (bod 73) a SpaceNet a Telekom Deutschland (bod 103). Viz rovněž body 63, 64 a 93 mého prvního stanoviska.

19 – V mém prvním stanovisku jsem tvrdil, že pojem „závažná trestná činnost“ je podle mého názoru třeba vykládat autonomně proto, aby se zabránilo jakémukoli obcházení požadavků stanovených v čl. 15 odst. 1 směrnice 2002/58 členskými státy. Na tomto názoru trvám. Musím však zdůraznit, že i kdyby Soudní dvůr rozhodl, že definice „závažné trestné činnosti“ je ponechána na členských státech, musela by být v každém případě stanovena v mezích unijního práva a nemohla by být rozšířena do té míry, že by toto ustanovení bylo zbaveno své podstaty.

50. Mechanismus odstupňované reakce umožňuje Hadopi spojit IP adresu osob podezřelých z toho, že použily svůj přístup k internetu k porušování autorského práva v *peer-to-peer* síti, sdělenou organizacemi zastupujícími nositele práv, s totožností této osoby, jakož i s výpisem ze souboru nahraného v rozporu s autorským právem. Jak uvedli Komise a EIOÚ na jednání, tyto prvky sice poskytují více informací než jen totožnost údajného porušovatele, avšak nevedou k velmi přesným závěrům o soukromém životě této osoby. Jak jsem totiž uvedl v mém prvním stanovisku[20], jedná se pouze o odhalení určitého prohlížení obsahu, které samo o sobě neumožňuje vytvořit podrobný profil osoby, která jej provedla.

51. To platí tím spíše, že zaprvé naprostá většina IP adres sdělených Hadopi jsou tzv. dynamické IP adresy, které jsou ze své podstaty proměnlivé a odpovídají určité identitě pouze v určitém časovém okamžiku, který se shoduje se zpřístupněním daného obsahu. Proto vylučují jakékoliv úplné sledování.

52. Zadruhé musím zdůraznit, že ochrana základních práv na internetu podle mého názoru nemůže odůvodňovat odepření přístupu k údajům týkajícím se IP adresy, obsahu díla a totožnosti osoby, která je zpřístupnila v rozporu s autorským právem, ale pouze to, že uchovávání těchto údajů a přístup k nim musí být doprovázeny ochrannými opatřeními. V tomto ohledu je výmluvná analogie s reálným světem: osoba podezřelá ze spáchání krádeže se nemůže dovolávat svého práva na ochranu soukromého života, aby zabránila osobám odpovědným za stíhání tohoto trestného činu dozvědět se o odcizeném obsahu. Naproti tomu se taková osoba může zcela oprávněně dovolávat svých základních práv, aby zamezila v průběhu řízení přístupu k širšímu souboru údajů, než jaký je nezbytný pro kvalifikaci údajného trestného činu.

53. Nakonec poznamenávám, že na rozdíl od tvrzení žalobců se nezdá, že by mechanismus odstupňované reakce zahrnoval všeobecný dohled nad uživateli *peer-to-peer* sítí. Cílem totiž není prověřit veškerou jejich činnost na dané síti, aby se zjistilo, zda zpřístupnili dílo v rozporu s autorským právem, ale spíše na základě souboru identifikovaného jako porušení práv určit držitele internetového přístupu, z něhož uživatel internetu dílo zpřístupnil. Stejně tak, jak EIOÚ zdůraznil na jednání, nejde o sledování činnosti všech uživatelů *peer-to-peer* sítí, ale pouze činnosti těch osob, které nahrávají soubory porušující práva, neboť nahrávání těchto souborů prozrazuje ještě méně o soukromém životě osoby, pokud je prováděno pouze proto, aby tito uživatelé internetu mohli stahovat následně jiné soubory.

54. Za těchto podmínek se mi zdá, že důvody, které vedly Soudní dvůr k tomu, aby považoval uchovávání IP adres a přístup k nim za závažný zásah do základních práv, se nevztahují na mechanismus odstupňované reakce, jak jej uplatňuje Hadopi. Z toho vyplývá, že závažnost zásahu, který s sebou nese takové uchovávání a přístup, by měla být při posuzování zásady proporcionality diferencována.

55. Jinými slovy, domnívám se, že judikatura Soudního dvora týkající se závažnosti zásahu do základních práv způsobeného uchováváním IP adres a přístupem k nim by neměla být vykládána v tom smyslu, že takový zásah je vždy závažným zásahem, ale že je tomu tak pouze v případě, kdy IP adresy mohou vést k úplnému sledování postupu prohlížení uživatelem internetu a k vyvození velmi přesných závěrů o jeho soukromém životě.

[20] – Bod 101 mého prvního stanoviska.

56. Jelikož tomu tak není v situaci, jako je situace dotčená v původním řízení, vyplývá z toho, že zásah spojený s uchováváním a přístupem k totožnostem odpovídajícím IP adrese použité ke zpřístupnění obsahu v rozporu s autorským právem by měl být odůvodnitelný cílem boje proti širší trestné činnosti, než je samotná závažná trestná činnost.

57. Mimoto upřesňuji, že zásah do základních práv, který je spojen s uchováváním a přístupem k údajům o totožnosti odpovídajícím IP adrese v takové situaci, o jakou se jedná v původním řízení, není zhoršen skutečností, že držitel internetového přístupu používaného ke zpřístupnění obsahu porušujícího práva není nutně osobou, která tento obsah zpřístupnila, takže doporučení Hadopi by mohlo vést k tomu, že by tomuto držiteli byl zpřístupněn obsah, který mohl být zpřístupněn třetí osobou. Zaprvé připomínám, že porušení, které Hadopi vyšetřuje, spočívá v porušení povinnosti zajistit, aby přístup nebyl používán ke zpřístupnění obsahu porušujícího autorská práva. Je proto nezbytné, aby informace potřebné k identifikaci obsahu porušujícího autorská práva byly zaslány údajnému porušovateli. Zadruhé, jak jsem již uvedl, jsem toho názoru, že informace týkající se dotčeného díla neumožňují vyvodit přesné závěry o soukromém životě osoby odpovědné za jeho zpřístupnění. Případné předání těchto informací držiteli internetového připojení tedy nepřekračuje rámec toho, co je nezbytné pro umožnění stíhání dotčeného porušení autorského práva.

b) Nezbytnost dotčených údajů pro odhalování a stíhání trestného činu

58. K tomu, aby byla zajištěna přiměřenost opatření týkajícího se uchovávání provozních údajů, jako jsou údaje o totožnosti odpovídající IP adrese, a přístupu k nim, přijatého podle čl. 15 odst. 1 směrnice 2002/58, je podle judikatury Soudního dvora třeba, aby byl zásah, který s sebou nese, omezen na to, co je nezbytně nutné k dosažení sledovaného cíle [21]. Zdá se mi, že právě o takový případ se jedná, pokud jde o opatření dotčené ve věci v původním řízení.

59. Jak jsem zdůraznil v mém prvním stanovisku [22], z téže judikatury Soudního dvora vyplývá, že v případě takového trestného činu spáchaného výhradně on-line, jako je porušení autorského práva na *peer-to-peer* síti, může IP adresa představovat jediný vyšetřovací prostředek umožňující identifikovat osobu, které byla tato adresa přidělena v okamžiku spáchání trestného činu [23]. Z toho podle mého názoru vyplývá, že uchovávání údajů o totožnosti odpovídajících IP adresám a přístup k nim za účelem odhalování a stíhání porušování autorských práv spáchaných on-line jsou v souladu s judikaturou nezbytně nutné k dosažení sledovaného cíle.

60. Je pravda, že každý požadavek na ochranu osobních údajů předpokládá omezení vyšetřovacích pravomocí. To vyplývá ze samotné zásady sladění protichůdných zájmů a takový výsledek nemůže být sám o sobě zpochybněn. Pokud je však IP adresa jediným prostředkem k identifikaci osoby podezřelé ze spáchání porušení práva duševního vlastnictví on-line, liší se taková situace od většiny trestních stíhání, u nichž Soudní dvůr uvádí, že „účinnost […] zpravidla nezávisí na jediném vyšetřovacím nástroji, nýbrž na všech vyšetřovacích nástrojích, které mají za tímto účelem k dispozici příslušné vnitrostátní orgány“ [24]. Pokud bychom připustili, že údaje o totožnosti odpovídající IP adresám nesmějí být v takové situaci, jako je situace dotčená ve věci v původním řízení, uchovávány a zpřístupňovány, nevedlo by to stejně jako v případě jakéhokoli

[21] – Rozsudky La Quadrature du Net a další (body 120 až 122 a 132), Commissioner of An Garda Síochána a další (body 48 a 54), jakož i SpaceNet a Telekom Deutschland (body 63 a 69).

[22] – Bod 78 mého prvního stanoviska.

[23] – Rozsudky La Quadrature du Net a další (bod 154), Commissioner of An Garda Síochána a další (bod 73) a SpaceNet a Telekom Deutschland (bod 100).

[24] – Rozsudek Commissioner of An Garda Síochána a další (bod 69).

opatření zajišťujícího ochranu provozních údajů k pouhému omezení vyšetřovacích pravomocí, ale zbavilo by to vnitrostátní orgány jediného prostředku k odhalování a stíhání určitých protiprávních jednání.

61. Jinými slovy, podle výkladu čl. 15 odst. 1 směrnice 2002/58, který navrhuji, se nejedná o to, aby bylo na základě přezkumu nezbytnosti takového opatření povoleno uchovávání údajů a přístup k nim, které pouze *usnadňují* odhalování a stíhání protiprávních jednání, pokud je lze odhalit a stíhat i konkurujícími prostředky, i když jsou méně účinné. Naproti tomu je třeba umožnit uchovávání takových údajů a přístup k nim, pokud jsou *nezbytné* pro identifikaci osoby podezřelé ze spáchání trestného činu, která by bez těchto prostředků nemohla být stíhána, neboť dotčené údaje jsou jediným prostředkem identifikace uživatele internetu, pokud je trestný čin spáchán výhradně on-line.

62. Podle mého názoru je třeba takový výklad použít, nechceme-li připustit, aby celá jedna oblast trestných činů byla vyloučena z trestního postihu [25].

63. Z výše uvedeného podle mého názoru vyplývá, že vnitrostátní právní úprava, která umožňuje poskytovatelům služeb elektronických komunikací uchovávat pouze údaje o totožnosti odpovídající IP adresám a správnímu orgánu mít k těmto údajům přístup, je plně přiměřená sledovanému cíli, a to stíhání porušování autorského práva a práv s ním souvisejících na internetu, pokud je zásah do základních práv, který s sebou nese, omezené závažnosti a pokud jsou tyto údaje jediným prostředkem vyšetřování umožňujícím identifikaci osoby, které byla tato adresa přidělena v okamžiku spáchání trestného činu.

64. Domnívám se proto, že čl. 15 odst. 1 směrnice 2002/58 je třeba vykládat tak, že takové právní úpravě nebrání.

2. K existenci náležitých hmotněprávních a procesních záruk

65. Pokud jde konkrétně o přístup k údajům o totožnosti odpovídajícím IP adresám, z judikatury Soudního dvora vyplývá, že samotná striktní přiměřenost opatření nestačí k tomu, aby toto opatření bylo slučitelné s čl. 15 odst. 1 směrnice 2002/58.

66. K tomu, aby bylo zajištěno, že přístup k provozním a lokalizačním údajům bude omezen na nezbytně nutné, totiž Soudní dvůr rozhodl, že je zásadní, aby tento přístup podléhal předchozímu přezkumu ze strany soudu nebo nezávislého správního orgánu, které mají veškeré pravomoci a vykazují všechny záruky nezbytné pro sladění jednotlivých oprávněných zájmů a dotčených práv [26].

67. Striktní výklad judikatury by tedy vedl k závěru, že přístup Hadopi k údajům o totožnosti odpovídajícím IP adresám osob podezřelých ze spáchání porušení autorského práva na internetu by měl podléhat takovému předchozímu přezkumu, který v současném mechanismu odstupňované reakce neexistuje.

[25] – Bod 81 mého prvního stanoviska. V tomto ohledu viz rovněž body 79 a násl. tohoto stanoviska.

[26] – Rozsudky Tele2 (bod 120); Prokuratuur (body 51 a 52), jakož i Commissioner of An Garda Síochána a další (body 106 a 107).

68. Jak však tvrdila irská vláda na jednání a jak jsem uvedl ve svém prvním stanovisku, domnívám se, že požadavek předchozího přezkumu soudem nebo nezávislým správním orgánem není systematickým požadavkem, ale závisí na komplexnější analýze daného opatření s přihlédnutím jak k závažnosti zásahu, který s sebou nese, tak i zárukám, jež stanoví.

69. Zdůrazňuji, že v každém z rozsudků, v nichž byl stanoven požadavek předchozího přezkumu soudem nebo nezávislým správním orgánem, se totiž jednalo o vnitrostátní právní úpravy, které umožňovaly přístup k veškerým provozním a lokalizačním údajům uživatelů týkajícím se všech prostředků elektronické komunikace uživatelů [27] nebo přinejmenším souvisejícím s pevnými telefonními linkami a mobilními telefony [28] určených uživatelů.

70. Z toho vyvozuji, že požadavek takového předchozího přezkumu se řídí závažností zásahu v dotčených věcech. Jak Soudní dvůr zdůraznil, jednalo se o údaje, na základě nichž „lze skutečně vyvodit přesné, ba dokonce velmi přesné závěry o soukromém životě osob […], tedy o každodenních zvyklostech, o místech, kde trvale či přechodně pobývají, o denních či jiných přesunech, o aktivitách, společenských vztazích těchto osob a o společenských kruzích, se kterými se stýkají“ [29]. Navíc se týkaly údajů osob, které již byly identifikovány a byly podezřelé ze spáchání trestného činu na základě jiných indicií, přičemž dotčené údaje umožnily posílit důkazy proti dotčenému uživateli rozšířením rozsahu údajů, které se ho týkají.

71. Pokud však jde o právní úpravu dotčenou ve věci v původním řízení a jak jsem již zdůraznil, závažnost zásahu, který předpokládá spojení údajů o totožnosti s IP adresou, je mnohem menší než zásah vyplývající z přístupu ke všem provozním a lokalizačním údajům osoby, neboť toto spojení neposkytuje žádné informace, které by umožnily vyvozovat přesné závěry o soukromém životě dotčené osoby.

72. Mimoto, jak jsem uvedl v prvním stanovisku [30], tyto údaje se týkají pouze osob, které se v návaznosti na objektivní zjištění užívání IP adresy v rozporu s autorským právem vyhotovené organizacemi zastupujícími nositele práv dopustily jednání, jež by mohlo představovat nesplnění povinnosti obezřetnosti stanovené v článku L. 336-3 CPI. Nejsou předem identifikovány žádným jiným způsobem, jelikož jediným prostředkem identifikace dotyčné osoby je spojení IP adresy s údaji o totožnosti. Přístup k těmto údajům tedy neumožňuje, jak tomu bylo v případech, o nichž Soudní dvůr rozhodoval dříve, získat dodatečné a přesné informace o činnosti osob, které již byly podezřelé na základě jiných skutečností, ale pouze umožnit použití IP adresy, která je jinak irelevantní. Za těchto podmínek jsou údaje, k nimž má Hadopi přístup, *de facto* omezené.

73. Podle mého názoru je zásadní rozdíl mezi přístupem k osobním údajům osoby podezřelé ze spáchání trestného činu za účelem prokázání její viny a takovým přístupem, který má umožnit odhalení totožnosti pachatele již zjištěného trestného činu.

74. Podle mého názoru je tomu tak tím spíše, že shromažďování IP adres v *peer-to-peer* sítích podléhá předchozímu povolení omezenému pouze na tyto údaje, takže Hadopi nemá nikdy k dispozici neomezený soubor údajů týkajících se uživatelů internetu podezřelých ze spáchání porušení autorských práv na internetu [31].

27 – Rozsudky Tele2 a Commissioner of An Garda Síochána a další.

28 – Rozsudek Prokuratuur.

29 – Rozsudek Prokuratuur (bod 36).

30 – Bod 102 mého prvního stanoviska.

31 – Bod 33 tohoto stanoviska.

75. Logika, z níž vychází požadavek předchozího přezkumu soudem nebo nezávislým správním orgánem, se tedy nepoužije na takový mechanismus odstupňované reakce, jako je mechanismus dotčený v původním řízení, takže takový požadavek nepovažuji za nutný k zajištění toho, aby zásah do základních práv, který s sebou nese tento mechanismus, byl omezen pouze na to, co je absolutně nezbytné.

76. Z výše uvedeného vyplývá, že vnitrostátní právní úprava umožňující uchovávání údajů o totožnosti odpovídajících IP adresám a přístup k nim ze strany takového nezávislého správního orgánu, jako je Hadopi, za účelem identifikace držitelů těchto adres podezřelých z porušování autorských práv, aniž tento přístup podléhá předchozímu přezkumu soudu nebo nezávislého správního orgánu, je v souladu se zásadami stanovenými judikaturou Soudního dvora, pokud tyto údaje představují jediný způsob identifikace osoby, které byla IP adresa přidělena v okamžiku spáchání trestného činu, takže čl. 15 odst. 1 směrnice 2002/58 musí být vykládán v tom smyslu, že takové právní úpravě nebrání.

77. Kromě těchto úvah týkajících se věci v původním řízení je třeba ještě učinit několik obecnějších poznámek k nutnosti dalšího vývoje judikatury Soudního dvora.

C. Nutný a omezený další vývoj judikatury

78. Vícero argumentů hovoří ve prospěch zjemnění judikatury Soudního dvora týkající se uchovávání takových údajů, jako jsou IP adresy, které se váží k údajům o totožnosti, a přístupu k nim.

79. Zaprvé, jak jsem již zdůraznil [32], v situaci dotčené ve věci v původním řízení je získání údajů o totožnosti odpovídajících IP adrese jediným vyšetřovacím prostředkem umožňujícím identifikovat osobu, jíž byla tato adresa přidělena v okamžiku spáchání dotčeného trestného činu.

80. Z toho nutně vyplývá, že pokud by Soudní dvůr rozhodl, že čl. 15 odst. 1 směrnice 2002/58 přesto brání jejich uchovávání a přístupu k nim, vnitrostátní orgány by *de facto* přišly o tento jediný prostředek identifikace a z téhož důvodu by pachatelé dotčených trestných činů nemohli být nikdy stíháni [33]. To mě vedlo k tomu, že jsem v mém prvním stanovisku upozornil na možnost systémové beztrestnosti tohoto trestného činu [34].

81. Riziko systémové beztrestnosti se neomezuje pouze na porušování autorského práva spáchaná v *peer-to-peer* sítích, ale vztahuje se, jak uvedla česká vláda na jednání, na všechna protiprávní jednání spáchaná výhradně on-line.

82. Protiprávní jednání, jejichž pachatel může být identifikován pouze prostřednictvím své IP adresy, by totiž nikdy nemohla být stíhána a předpisy, které je postihují, by se nikdy nepoužily, pokud by bylo rozhodnuto, že jak uchovávání údajů, tak přístup k nim jsou v rozporu s unijním právem.

83. V tomto ohledu poznamenávám, že je pravda, jak uvedli žalobci v původním řízení, že identifikaci pachatelů některých protiprávních jednání spáchaných výhradně on-line by teoreticky mohly umožnit jiné prostředky. Odkazují tak zejména na identifikátor používaný na

[32] – Bod 59 tohoto stanoviska.

[33] – Bod 62 tohoto stanoviska.

[34] – Body 78 a násl. mého prvního stanoviska.

sociálních sítích a na údaje spojené s účtem uživatele, e-mailovou adresou, telefonním číslem nebo aspektem jeho soukromého života, který tato osoba odhalila. K tomu, aby bylo možné tyto údaje propojit s identitou osoby, je však zapotřebí hloubkové šetření, během něhož se zkoumá on-line činnost uživatele internetu. Zdá se mi tedy, že použití těchto vyšetřovacích prostředků může umožnit vyvození velmi přesných závěrů o soukromém životě osob, na rozdíl od pouhé IP adresy, takže uchovávání těchto údajů a přístup k nim by v tomto smyslu byly v rozporu s čl. 15 odst. 1 směrnice 2002/58.

84. Za těchto podmínek není přístup k údajům o totožnosti odpovídajícím IP adrese uživatele internetu jistě jediným teoretickým prostředkem vyšetřování, který umožňuje identifikovat osobu, jíž tato adresa patřila v okamžiku spáchání trestného činu, ale je jediným prostředkem umožňujícím trestní stíhání, který s sebou nese nejmenší zásah do základních práv této osoby, a tudíž zabraňuje obecné beztrestnosti.

85. Zadruhé znovu zdůrazňuji, že takové řešení by podle mého názoru umožnilo sladit dvě linie judikatury Soudního dvora, které jsou zdrojem určitého napětí, jež jsem identifikoval v mém prvním stanovisku [35] a ve stanovisku ve věci M. I. C. M. [36], a sice zaprvé judikaturu týkající se uchovávání údajů a přístupu k nim a zadruhé judikaturu týkající se sdělování IP adres přidělených zdroji připojení v rámci žalob na ochranu práv duševního vlastnictví podaných soukromými osobami.

86. Zatřetí ačkoli je třeba uvítat judikaturu Soudního dvora od vydání rozsudků Tele2 a La Quadrature du Net a další, neboť umožnila vytvořit rámec pro ochranu základních práv uživatelů služeb elektronických komunikací, tato judikatura je nicméně poznamenána určitou kazuistikou. V průběhu přezkumu věcí, které mu byly předloženy, totiž Soudní dvůr postupně zpřesňoval svou judikaturu, což mu umožnilo přezkoumat různé vnitrostátní právní úpravy ve světle čl. 15 odst. 1 směrnice 2002/58. Soudní dvůr však není schopen předjímat potenciálně všechna opatření, která by mohla být analyzována ve světle tohoto ustanovení. O tom ostatně svědčí množství žádostí o rozhodnutí o předběžné otázce [37], které Soudní dvůr obdržel od vydání rozsudku Tele2, což podle mého názoru svědčí o obtížích, které mohou mít vnitrostátní soudy při uplatňování zásad stanovených v judikatuře Soudního dvora na situace odlišné od těch, v nichž byly vydány dotčené rozsudky [38].

[35] – Body 69 a násl. mého prvního stanoviska.

[36] – C-597/19, EU:C:2020:1063.

[37] – Rozsudky ze dne 2. října 2018, Ministerio Fiscal (C-207/16, EU:C:2018:788); La Quadrature du Net a další; Prokuratuur; Commissioner of An Garda Síochána a další, jakož i SpaceNet a Telekom Deutschland.

[38] – V tomto ohledu může rostoucí počet žádostí o rozhodnutí o předběžné otázce týkajících se výkladu čl. 15 odst. 1 směrnice 2002/58 rovněž naznačovat určitou zdrženlivost vnitrostátních soudů při uplatňování zásad stanovených Soudním dvorem na mírně odlišné situace, a to z důvodu specifických rysů vnitrostátních právních řádů. V tomto ohledu viz zejména Cameron, I., „Metadata retention and national security: Privacy international and La Quadrature du Net“, *Common Market Law Review*, 2021, sv. 58, č. 5, s. 1433 až 1471, nebo dále Bertrand, B., „L'audace sans le tact: jusqu'où la Cour de justice peut-elle aller trop loin?“, *Dalloz IP/IT*, 2021, č. 9, s. 468 až 472. Zdá se mi proto, že pro zachování plodného dialogu mezi Soudním dvorem a soudy členských států je o to důležitější, aby se Soudní dvůr mohl přizpůsobit, pokud to okolnosti vyžadují. Jak uvedli autoři právní nauky, vysoký standard ochrany zavedený judikaturou Soudního dvora nemůže být skutečně účinný bez podpory vnitrostátních soudů, které jsou primárně odpovědné za jeho provádění. V tomto ohledu viz zejména Teyssedre, J., „Strictly regulated retention and access regimes for metadata: Commissioner of An Garda Siochana“, *Common Market Law Review*, sv. 60, č. 2, 2023, s. 569 až 588, a Sirinelli, J., „La protection des données de connexion par la Cour de justice: cartographie d'une jurisprudence européenne inédite“, *revue trimestrielle de droit européen*, sv. 57, č. 2, 2021, s. 313 až 329.

87. Z toho tedy vyplývá, že považuji za nezbytnou určitou míru flexibility, pokud jsou Soudnímu dvoru předkládána k přezkumu taková opatření, která nemohla být v předchozích rozsudcích předpokládána, jako jsou právní úpravy týkající se protiprávních jednání, která lze stíhat pouze tehdy, pokud jsou uchovávány a zpřístupňovány údaje o totožnosti odpovídající IP adresám, kterými se Soudní dvůr dosud nezabýval.

88. Nejde tedy o to, jak obhajovala dánská vláda, přehodnotit judikaturu Soudního dvora, ale připustit, že na základě zásad, z nichž vychází, lze za velmi omezených okolností nalézt diferencovanější řešení.

89. Výklad čl. 15 odst. 1 směrnice 2002/58, který navrhuji, totiž umožňuje uchovávání údajů o totožnosti odpovídajících IP adresám a přístup k nim pouze za účelem stíhání trestných činů, jejichž pachatelé by bez těchto údajů nemohli být identifikováni. Vztahuje se tedy výhradně na protiprávní jednání, k nimž došlo výhradně na internetu a nezpochybňuje řešení nalezená v judikatuře týkající se uchovávání širších údajů a přístupu k nim, která sledují jiné cíle.

V. Závěry

90. S ohledem na všechny výše uvedené úvahy navrhuji Soudnímu dvoru, aby na předběžné otázky položené Conseil d'État (Státní rada, Francie) odpověděl následovně:

„Článek 15 odst. 1 směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (směrnice o soukromí a elektronických komunikacích), ve znění směrnice Evropského parlamentu a Rady 2009/136/ES ze dne 25. listopadu 2009, ve spojení s články 7, 8 a 11, jakož i čl. 52 odst. 1 Listiny základních práv Evropské unie,

musí být vykládán v tom smyslu, že

nebrání vnitrostátní právní úpravě, která umožňuje poskytovatelům služeb elektronických komunikací uchovávání a správnímu orgánu pověřenému ochranou autorských práv a práv souvisejících s právem autorským proti porušování těchto práv na internetu přístup omezený na údaje o totožnosti odpovídající IP adresám, aby tento orgán mohl identifikovat držitele těchto IP adres, kteří jsou podezřelí z tohoto porušování, a případně vůči nim mohl přijmout odpovídající opatření, aniž tento přístup podléhá předchozímu přezkumu ze strany soudu nebo nezávislého správního orgánu, jsou-li tyto údaje jediným prostředkem vyšetřování umožňujícím identifikovat osobu, které byla tato adresa přidělena v okamžiku spáchání trestného činu.“