Zbierka súdnych rozhodnutí

NÁVRHY GENERÁLNEHO ADVOKÁTA
MACIEJ SZPUNAR
prednesené 28. septembra 2023 [1]

Vec 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

[návrh na začatie prejudiciálneho konania, ktorý podala Conseil d'État (Štátna rada, Francúzsko)]

„Návrh na začatie prejudiciálneho konania – Spracúvanie osobných údajov a ochrana súkromia v sektore elektronických komunikácií – Smernica 2002/58/ES – Článok 15 ods. 1 – Možnosť členských štátov obmedziť rozsah určitých práv a povinností – Povinnosť predchádzajúceho preskúmania zo strany súdu alebo nezávislého správneho orgánu s donucovacou právomocou – Údaje o totožnosti zodpovedajúce IP adrese"

I. Úvod

1. Súdny dvor v nadväznosti na žiadosť veľkej komory predloženú podľa článku 60 ods. 3 Rokovacieho poriadku Súdneho dvora rozhodol 7. marca 2023 o postúpení tejto veci plénu.

2. Uznesením z 23. marca 2023 Súdny dvor (plénum) rozhodol o opätovnom začatí ústnej časti konania a vyzval zainteresované strany uvedené v článku 23 Štatútu Súdneho dvora Európskej únie, Európskeho dozorného úradníka pre ochranu údajov (EDPS) a Agentúru Európskej únie pre sieťovú a informačnú bezpečnosť (ENISA), aby sa zúčastnili na novom pojednávaní.

3. Dňa 27. októbra 2022 som predniesol svoje prvé návrhy v tejto veci pred skončením ústnej časti konania. Tieto nové závery sú teda pre mňa príležitosťou doplniť niektoré moje úvahy v tejto veci o zásadné otázky súvisiace s uchovávaním a prístupom k osobným údajom.

[1] Jazyk prednesu: francúzština.

II. Právny rámec

A. Právo Únie

4. Odôvodnenia 2, 6, 7, 11, 22, 26 a 30 smernice 2002/58/ES [2] uvádzajú:

„(2) Táto smernica sa snaží rešpektovať základné práva a dodržiavať princípy uznané najmä chartou základných práv Európskej únie [(ďalej len ‚Charta')]. Táto smernica sa snaží najmä o plné zabezpečenie práv stanovených v článkoch 7 a 8 uvedenej charty.

…

(6) Internet revolucionalizoval tradičné trhové štruktúry tým, že poskytuje spoločnú, globálnu infraštruktúru pre ponuku širokého rozsahu elektronických komunikačných služieb. Verejne dostupné elektronické komunikačné služby na internete otvárajú nové možnosti pre užívateľov, no prinášajú aj nové riziká pre ich osobné údaje a súkromie.

(7) V prípade verejných komunikačných sietí by sa mali stanoviť špecifické právne, regulačné a technické opatrenia, aby boli chránené základné práva a slobody fyzických osôb a legitímne záujmy právnických osôb, najmä z hľadiska zvyšovania kapacity automatického uchovávania a spracovávania údajov týkajúcich sa účastníkov a užívateľov.

…

(11) Podobne ako smernica [95/46/ES [3]] sa táto smernica netýka otázok ochrany základných práv a slobôd vzťahujúcich sa k činnostiam, ktoré nie sú upravené právom spoločenstva. Preto nemení existujúcu rovnováhu medzi právami jednotlivca na súkromie a možnosťami členských štátov prijať opatrenia uvedené v článku 15 ods. 1 tejto smernice, ktoré sú potrebné na ochranu verejnej bezpečnosti, obrany, bezpečnosti štátu (vrátane ekonomického blahobytu štátu, keď sa činnosti týkajú záležitostí bezpečnosti štátu) a presadzovanie trestného práva. Následne táto smernica nemá vplyv na možnosť členských štátov zachytávať elektronické správy alebo prijímať iné opatrenia, ak je to nevyhnutné z akýchkoľvek iných dôvodov a v súlade s Európskym dohovorom na ochranu ľudských práv a základných slobôd [podpísaným v Ríme 4. novembra 1950], interpretovaným rozsudkami súdneho dvora týkajúcimi sa ľudských práv [Európskeho súdu pre ľudské práva – *neoficiálny preklad*]; také opatrenia musia byť primerané, prísne proporcionálne vo vzťahu k zamýšľanému účelu a potrebné v rámci demokratickej spoločnosti a mali by byť predmetom primeranej ochrany v súlade s Európskym dohovorom na ochranu ľudských práv a základných slobôd.

…

[2] Smernica Európskeho parlamentu a Rady z 12. júla 2002, týkajúca sa spracovávania osobných údajov a ochrany súkromia v sektore elektronických komunikácií (smernica o súkromí a elektronických komunikáciách) (Ú. v. ES L 201, 2002, s. 37; Mim. vyd. 13/029, s. 514), zmenená smernicou Európskeho parlamentu a Rady 2009/136/ES z 25. novembra 2009 (Ú. v. EÚ L 337, 2009, s. 11) (ďalej len „smernica 2002/58").

[3] Smernica Európskeho parlamentu a Rady z 24. októbra 1995 o ochrane fyzických osôb pri spracovaní osobných údajov a voľnom pohybe týchto údajov (Ú. v. ES L 281, 1995, s. 31; Mim. vyd. 13/015, s. 355).

(22) Zákaz ukladania správ a príslušných prevádzkových dát [príslušných údajov o prenose dát – *neoficiálny preklad*] osobami inými, než sú užívatelia alebo účastníci bez ich súhlasu, nie je určený na zákaz akéhokoľvek automatického, dočasného a prechodného uloženia týchto informácií, pokiaľ sa to uskutočňuje výhradne na účely výkonu prenosu v elektronickej komunikačnej sieti a za predpokladu, že informácie sa neukladajú na dobu dlhšiu, než je nevyhnutné na prenos a riadenie chodu prenosu a že počas doby uloženia je zaručená dôvernosť informácií. …

…

(26) Údaje vzťahujúce sa k účastníkom, ktoré sú spracovávané v elektronickej komunikačnej sieti a slúžia na zabezpečenie spojenia a prenos informácií, obsahujú údaje o súkromnom živote fyzických osôb a týkajú sa práva na rešpektovanie ich korešpondencie alebo sa týkajú legitímnych záujmov právnických osôb; také údaje sa môžu ukladať len v rozsahu, aký je potrebný na zabezpečenie služby na účely fakturácie a poplatkov za spojenie a len na limitovanú dobu; akékoľvek ďalšie spracovávanie takých údajov…, sa môže povoliť len vtedy, keď účastník s týmto súhlasí na základe úplných a presných informácií poskytovateľa verejne dostupných elektronických komunikačných služieb o druhu ďalšieho spracovania, ktoré zamýšľa vykonať a o právach účastníka nedať alebo odvolať svoj súhlas na také spracovanie;…

…

(30) Systémy poskytovania elektronických komunikačných sietí a služieb by mali byť konštruované tak, aby bol obmedzený počet nevyhnutných osobných údajov na minimum. …“

5. Článok 2 tejto smernice, nazvaný „Definície“, stanovuje:

„…

Platia aj tieto definície:

a) ‚užívateľ‘ znamená každú fyzickú osobu, ktorá používa verejne dostupnú elektronickú komunikačnú službu na súkromné alebo obchodné účely bez toho, aby si túto službu predplatil;

b) ‚prevádzkové dáta [údaje o prenose dát – *neoficiálny preklad*]‘ znamenajú akékoľvek údaje spracovávané na účely prenosu správy v elektronickej komunikačnej sieti alebo na účely fakturácie prenosu;

c) ‚lokalizačné dáta [údaje o polohe – *neoficiálny preklad*]‘ znamenajú akékoľvek údaje spracúvané v elektronickej komunikačnej sieti alebo prostredníctvom elektronickej komunikačnej služby, udávajúce geografickú polohu koncového zariadenia užívateľa verejne dostupnej elektronickej komunikačnej služby;

d) ‚správa‘ znamená akékoľvek informácie vymieňané alebo prenášané medzi konečným počtom účastníkov pomocou verejne dostupnej elektronickej komunikačnej služby. Toto nezahŕňa akékoľvek informácie prenášané ako časť rozhlasových služieb pre verejnosť v elektronickej komunikačnej sieti, pokiaľ sa informácie nemôžu spájať s identifikovateľným účastníkom alebo užívateľom prijímajúcim informácie;

…“

6. Článok 3 uvedenej smernice, nazvaný „Dotknuté služby“, stanovuje:

„Táto smernica sa vzťahuje na spracúvanie osobných údajov v súvislosti s poskytovaním verejne dostupných elektronických komunikačných služieb vo verejných komunikačných sieťach v Spoločenstve vrátane verejných komunikačných sietí, ktoré podporujú zariadenia na zber údajov a identifikáciu.“

7. Článok 5 tej istej smernice s názvom „Dôvernosť správy“ stanovuje:

„1. Členské štáty vnútroštátnymi právnymi predpismi zabezpečia dôvernosť správ a príslušných prevádzkových dát [príslušných údajov o prenose dát – *neoficiálny preklad*] prenášaných pomocou verejnej komunikačnej siete a verejne dostupných elektronických komunikačných sietí. Zakážu najmä počúvanie, odpočúvanie a iné druhy narušovania alebo dohľadu nad správami a príslušnými prevádzkovými dátami [príslušnými údajmi o prenose dát – *neoficiálny preklad*] zo strany iných osôb[,] než sú užívatelia[,] bez súhlasu príslušných užívateľov, pokiaľ to nie je zákonne oprávnené v súlade s článkom 15 ods. 1 Tento odsek nebráni technickému uloženiu, ak je to potrebné s cieľom prenosu správy, bez vplyvu na princíp dôvernosti.

…

3. Členské štáty zabezpečia, aby sa ukladanie informácií alebo získavanie prístupu k informáciám, ktoré už boli uložené, v koncovom zariadení účastníka alebo užívateľa povolilo len pod podmienkou, že dotknutý účastník alebo užívateľ dal na to vopred súhlas na základe jasných a komplexných informácií v súlade so smernicou [95/46], okrem iného aj o účeloch spracovania. To nebráni nijakému technickému uloženiu ani prístupu výhradne na účely výkonu prenosu správy prostredníctvom elektronickej komunikačnej siete alebo ak je to nevyhnutne potrebné na to, aby poskytovateľ služieb informačnej spoločnosti, ktoré si účastník alebo užívateľ výslovne vyžiadal, mohol tieto služby poskytnúť.“

8. Článok 6 smernice 2002/58, nazvaný „Prevádzkové údaje [Údaje o prenose dát – *neoficiálny preklad*]“, stanovuje:

„1. Prevádzkové dáta [Údaje o prenose dát – *neoficiálny preklad*] týkajúce sa účastníkov a užívateľov, spracovávané a uložené poskytovateľom verejnej komunikačnej siete alebo verejne dostupnej elektronickej komunikačnej služby, sa musia vymazať alebo zanonymniť [anonymizovať – *neoficiálny preklad*], ak už naďalej nie sú potrebné na účely prenosu správy, bez vplyvu na odseky 2, 3 a 5 tohto článku a článku 15 ods. 1.

2. Prevádzkové dáta [Údaje o prenose dát – *neoficiálny preklad*] potrebné na účely fakturácie účastníka a platby za spojenie sa môžu spracovávať. Také spracovanie je povolené len do konca obdobia, počas ktorého môže byť faktúra právne napadnutá alebo sa môže uplatniť nárok na platbu.

…“

9. Článok 15 tejto smernice, nazvaný „Uplatňovanie niektorých ustanovení smernice [95/46]“, v odseku 1 uvádza:

„Členské štáty môžu prijať legislatívne opatrenia na obmedzenie rozsahu práv a povinností uvedených v článku 5, článku 6, článku 8 ods. 1, 2, 3 a 4 a článku 9 tejto smernice, ak také obmedzenie predstavuje nevyhnutné, vhodné a primerané opatrenie v demokratickej spoločnosti na zabezpečenie národnej bezpečnosti (t. j. bezpečnosti štátu), obrany, verejnej bezpečnosti a na zabránenie, vyšetrovanie, odhaľovanie a stíhanie trestných činov alebo neoprávnené používanie [neoprávneného používania – *neoficiálny preklad*] elektronického komunikačného systému podľa článku 13 ods. 1 smernice [95/46]. Na tento účel členské štáty môžu, medzi iným, prijať legislatívne opatrenia umožňujúce zadržanie [uchovávanie – *neoficiálny preklad*] údajov na limitované obdobie, oprávnené z dôvodov stanovených v tomto odseku. Všetky opatrenia uvedené v tomto odseku musia byť v súlade so všeobecnými princípmi práva [Únie] vrátane tých, ktoré sú uvedené v článku 6 ods. 1 a 2 [ZEÚ].“

B. Francúzske právo

1. Zákonník duševného vlastníctva

10. Článok L. 331-12 code de la propriété intellectuelle (Zákonník duševného vlastníctva) v znení uplatniteľnom na spor vo veci samej (ďalej len „CPI“) stanovuje:

„Haute Autorité pour la diffusion des œuvres et la protection des droits sur Internet [Vysoký úrad pre šírenie diel a ochranu práv na internete; ďalej len ‚Hadopi‘] je nezávislý verejný orgán.“

11. Článok L. 331-13 CPI stanovuje:

„[Hadopi] zabezpečuje:

…

2° Úlohu ochrany [diel a predmetov, s ktorými je spojené autorské právo alebo s ním súvisiace právo v elektronických komunikačných sieťach] pred porušovaním týchto práv, ku ktorému dochádza v elektronických komunikačných sieťach používaných na poskytovanie komunikačných služieb online;…“

12. Podľa článku L. 331-15 tohto zákonníka:

„[Hadopi] sa skladá z kolégia a komisie na ochranu práv. …

…

Členovia kolégia a komisie na ochranu práv pri výkone svojich právomocí neprijímajú pokyny od žiadneho orgánu.“

13. Článok L. 331-17 uvedeného zákonníka stanovuje:

„Komisia na ochranu práv je zodpovedná za prijatie opatrení stanovených v článku L. 331-25.“

14. Podľa článku L. 331-21 toho istého zákonníka:

„[Hadopi] má na účely výkonu právomocí komisie na ochranu práv k dispozícii prísažných štátnych zamestnancov, ktorých poveruje predseda tohto úradu v súlade s podmienkami stanovenými dekrétom prijatom po stanovisku Conseil d'État [Štátna rada]. …

Členovia komisie na ochranu práv a zamestnanci uvedení v prvom odseku prijímajú podania adresované uvedenej komisii za podmienok stanovených v článku L. 331-24. Následne preskúmavajú skutkové okolnosti.

Na účely konania sú oprávnení získavať všetky dokumenty, na akomkoľvek nosiči, vrátane údajov uchovávaných a spracúvaných prevádzkovateľmi elektronických komunikácií podľa článku L. 34-1 code des postes et des communications électroniques [Zákonník pôšt a elektronických komunikácií] a poskytovateľmi uvedenými v článku 6 ods. I bodoch 1 a 2 loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique [zákon č. 2004-575 z 21. júna 2004 o podpore dôvery v digitálne hospodárstvo].

Môžu tiež získať kópie dokumentov uvedených v predchádzajúcom odseku.

Od prevádzkovateľov elektronických komunikácií môžu získať najmä totožnosť, poštovú adresu, elektronickú adresu a telefónne číslo účastníka, ktorého prístup k verejným komunikačným službám online bol využívaný na účely rozmnožovania, zobrazovania, sprístupňovania alebo verejného prenosu chránených diel alebo predmetov bez súhlasu nositeľov práv…, pokiaľ sa vyžaduje."

15. Článok L. 331-24 CPI stanovuje:

„Komisia na ochranu práv koná na základe podnetov prísažných a poverených zamestnancov, ktorých vymenúvajú:

– riadne založené organizácie zastupujúce profesijné záujmy,

– organizácie kolektívnej správy práv,

– Centre national du cinéma et de l'image animée [Národné centrum pre film a animovanú tvorbu].

Komisia na ochranu práv môže konať aj na základe informácií, ktoré jej poskytol prokurátor republiky.

Nemôže sa zaoberať skutkami spred viac ako šesť mesiacov."

16. Článok L. 331-25 tohto zákonníka, ktorý upravuje tzv. postup „odstupňovanej reakcie", stanovuje:

„Ak sa komisia na ochranu práv dozvie o skutkoch, ktoré môžu predstavovať porušenie povinnosti vymedzenej v článku L. 336-3 [CPI], môže poslať účastníkovi… odporúčanie, v ktorom mu pripomenie ustanovenia článku L. 336-3, pričom ho vyzve na dodržiavanie povinnosti vymedzenej v týchto ustanoveniach a upovedomí ho o hroziacich sankciách podľa článkov L. 335-7 a L. 335-7-1. Toto odporúčanie obsahuje tiež informácie pre účastníka o legálnej ponuke

kultúrneho obsahu online, o existencii bezpečnostných prostriedkov na zabránenie porušovania povinnosti vymedzenej v článku L. 336-3 a o nebezpečenstvách, ktoré pre obnovu umeleckej tvorby a ekonomiku kultúrneho sektora predstavujú postupy nerešpektujúce autorské právo a s ním súvisiace práva.

V prípade, že sa v lehote šiestich mesiacov od zaslania odporúčania uvedeného v prvom odseku zopakujú skutky, ktoré môžu predstavovať porušenie povinnosti vymedzenej v článku L. 336-3, môže komisia zaslať nové odporúčanie obsahujúce rovnaké informácie ako predchádzajúce odporúčanie zaslané elektronicky… K tomuto odporúčaniu musí pripojiť doporučený list s doručenkou alebo akýkoľvek iný prostriedok vhodný na preukázanie dátumu doručenia tohto odporúčania.

V odporúčaniach zaslaných na základe tohto článku sa uvedie dátum a čas, kedy boli zistené skutky, ktoré môžu predstavovať porušenie povinnosti vymedzenej v článku L. 336-3. Na druhej strane nesprístupňujú obsah chránených diel alebo predmetov, ktorých sa toto porušenie týka. Uvádzajú sa v nich telefónne, poštové a elektronické kontaktné údaje, na ktoré môže ich adresát, ak si to želá, podať pripomienky komisii na ochranu práv a získať, ak o to výslovne požiada, podrobnosti o obsahu chránených diel alebo predmetov dotknutých porušením povinnosti, ktoré sa mu vytýka.“

17. Článok L. 331-29 uvedeného zákonníka stanovuje:

„[Hadopi] je oprávnený vytvoriť automatizované spracúvanie osobných údajov osôb, ktoré sú predmetom konania podľa tohto pododdielu.

Účelom tohto spracúvania je umožniť komisii na ochranu práv vykonať opatrenia stanovené v tomto pododdiele, všetky súvisiace procesné úkony a spôsoby informovania organizácií zastupujúcich profesijné záujmy a organizácií kolektívnej správy práv o prípadných podaniach na súdny orgán, ako aj o oznámeniach uvedených v článku L.335-7 piatom odseku.

Dekrét… stanovuje podmienky uplatňovania tohto článku. Spresňuje najmä:

– kategórie zaznamenaných údajov a dobu ich uchovávania,

– príjemcov oprávnených prijímať oznámenia o týchto údajoch, najmä osoby, ktorých činnosť spočíva v poskytovaní prístupu k verejným komunikačným službám online,

– podmienky, za ktorých môžu dotknuté osoby uplatniť na [úrade Hadopi] svoje právo na prístup k údajom, ktoré sa ich týkajú…“

18. Článok L. 331-37 toho istého zákonníka stanovuje:

„Prevádzkovatelia elektronických komunikácií… a poskytovatelia… sú povinní prostredníctvom prepojenia na automatizované spracúvanie osobných údajov uvedené v článku L. 331-29 alebo použitím pamäťového média zaisťujúceho ich integritu a bezpečnosť oznamovať osobné údaje a informácie stanovené v bode 2 prílohy k [décret nº 2010-236 du 5 mars 2010 relatif au traitement automatisé des 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“ (dekrét č. 2010-236 z 5. marca 2010 o automatizovanom spracúvaní osobných údajov povolenom článkom

L. 331-29 [CPI] s názvom ‚Systém riadenia opatrení na ochranu diel na internete‘)[4] (ďalej len ‚dekrét z 5. marca 2010‘)]… v lehote do ôsmich dní od prenosu technických údajov komisiou na ochranu práv potrebných na identifikáciu účastníka, ktorého prístup k verejným online komunikačným službám bol použitý na účely rozmnožovania, zobrazovania, sprístupňovania alebo verejného prenosu chránených diel alebo predmetov bez súhlasu nositeľov práv…, pokiaľ sa vyžaduje.

…“

19. Článok R. 335-5 CPI stanovuje:

„I.- Za hrubú nedbanlivosť, ktorú možno potrestať pokutou stanovenou za priestupky piatej triedy, sa považuje skutočnosť, že osoba, ktorá poskytuje prístup k verejným komunikačným službám online, bez oprávneného dôvodu, ak sú splnené podmienky stanovené v odseku II:

1° nezaviedla prostriedok na zabezpečenie tohto prístupu; alebo

2° neprejavila náležitú starostlivosť pri zavedení tohto prostriedku.

II.- Ustanovenia odseku I sa uplatnia, len ak sú splnené tieto dve podmienky:

1° Podľa článku L. 331-25 a vo forme stanovenej v tomto článku komisia na ochranu práv odporúčala poskytovateľovi prístupu, aby zaviedol prostriedok na zabezpečenie svojho prístupu, ktorý umožňuje zabrániť jeho opätovnému využívaniu na účely rozmnožovania, zobrazovania, sprístupňovania alebo verejného prenosu diel alebo predmetov chránených autorským právom alebo s ním súvisiacim právom bez súhlasu nositeľov práv…, pokiaľ sa vyžaduje;

2° V priebehu jedného roka od predloženia tohto odporúčania sa tento prístup znovu použije na účely uvedené v bode 1 tohto odseku II.“

20. Článok L. 336-3 tohto zákonníka uvádza:

„Osoba, ktorá poskytuje prístup k verejným komunikačným službám online je povinná zabezpečiť, aby sa tento prístup nevyužíval na účely rozmnožovania, zobrazovania, sprístupňovania alebo verejného prenosu diel alebo predmetov chránených autorským právom alebo s ním súvisiacim právom bez súhlasu nositeľov práv…, pokiaľ sa vyžaduje.

Porušenie povinnosti vymedzenej v prvom odseku zo strany osoby, ktorá poskytuje prístup, nemá za následok vznik trestnej zodpovednosti dotknutej osoby…“

2. Dekrét z 5. marca 2010

21. Dekrét z 5. marca 2010 v znení uplatniteľnom na skutkové okolnosti sporu vo veci samej v článku 1 stanovuje:

„Účelom spracúvania osobných údajov s názvom ‚Systém riadenia opatrení na ochranu diel na internete‘ je, že komisia na ochranu práv [úradu Hadopi] vykonáva:

[4] JORF zo 7. marca 2010, text č. 19.

1° opatrenia stanovené v knihe III legislatívnej časti [CPI] (hlava III kapitola I oddiel 3 pododdiel 3) a knihe III regulačnej časti toho istého zákonníka (hlava III kapitola I oddiel 2 pododdiel 2);

2° podania prokurátorovi republiky o skutkoch, ktoré môžu predstavovať porušenia stanovené v článkoch L. 335-2, L. 335-3, L. 335-4 a R. 335-5 toho istého zákonníka, ako aj informovanie organizácií zastupujúcich profesijné záujmy a organizácií kolektívnej správy práv o týchto podaniach;

…“

22. Článok 4 tohto dekrétu stanovuje:

„I.- K osobným údajom a informáciám uvedeným v prílohe k tomuto dekrétu majú priamy prístup prísažní štátni zamestnanci poverení predsedom [úradu Hadopi] podľa článku L. 331-21 [CPI] a členovia komisie na ochranu práv uvedenej v článku 1.

II.- Prevádzkovatelia elektronických komunikácií a poskytovatelia uvedení v bode 2 prílohy k tomuto dekrétu sú príjemcami:

– technických údajov potrebných na identifikáciu účastníka,

– odporúčaní uvedených v článku L. 331-25 [CPI] s cieľom elektronicky ich zaslať svojim účastníkom,

– informácií potrebných na výkon doplňujúcich trestov pozastavenia prístupu k verejnej komunikačnej službe online, na ktoré komisiu na ochranu práv upozorňuje prokurátor republiky,

III.- Organizácie zastupujúce profesijné záujmy a organizácie kolektívnej správy práv sú príjemcami informácií o podaniach prokurátorovi republiky.

IV.- Súdne orgány sú príjemcami zápisníc o zistení skutkov, ktoré môžu predstavovať porušenia stanovené v článkoch L. 335-2, L. 335-3, L. 335-4, L. 335-7, R. 331-37, R. 331-38 a R. 335-5 [CPI].

O výkone trestu pozastavenia je informovaný automatizovaný register trestov.“

23. Príloha k dekrétu z 5. marca 2010 stanovuje:

„Osobné údaje a informácie zaznamenané pri spracúvaní s názvom ‚Systém riadenia opatrení na ochranu diel na internete‘ sú tieto:

1° Osobné údaje a informácie pochádzajúce od riadne založených organizácií zastupujúcich profesijné záujmy, organizácií kolektívnej správy práv, Národného centra pre film a animovanú tvorbu, ako aj od prokurátora republiky:

Pokiaľ ide o skutky, ktoré môžu predstavovať porušenie povinnosti vymedzenej v článku L. 336-3 [CPI]:

dátum a čas skutkov;

IP adresy dotknutých účastníkov;

použitý protokol vzájomného sprístupňovania (peer-to-peer);

pseudonym používaný účastníkom;

informácie o chránených dielach alebo predmetoch, ktorých sa skutky týkajú;

názov súboru, ako sa nachádza v zariadení účastníka (ak je k dispozícii);

poskytovateľ prístupu na internet, u ktorého bol prístup vytvorený alebo ktorý poskytol technický zdroj IP.

…

2° Osobné údaje a informácie o účastníkovi získané od prevádzkovateľov elektronických komunikácií… a poskytovateľov…:

priezvisko, krstné mená;

poštová adresa a e-mailové adresy;

telefónne kontaktné údaje;

adresa telefónneho zariadenia účastníka;

poskytovateľ prístupu na internet, ktorý využíva technické prostriedky poskytovateľa prístupu uvedeného v bode 1 a s ktorým účastník uzavrel zmluvu; číslo spisu;

dátum začiatku pozastavenia prístupu k verejnej komunikačnej službe online.

…“

3. Zákonník pôšt a elektronických komunikácií

24. Článok L. 34-1 code des postes et des communications électroniques (Zákonník pôšt a elektronických komunikácií) v znení článku 17 zákona č. 2021-998 z 30. júla 2021 [5] v odseku IIa stanovuje:

„Prevádzkovatelia elektronických komunikácií sú povinní uchovávať

[5] JORF z 31. júla 2021, text č. 1. Toto znenie článku L. 34 -1 tohto zákonníka, účinné od 31. júla 2021, bolo prijaté v nadväznosti na rozhodnutie Conseil d'État (Štátna rada, Francúzsko) z 21. apríla 2021, č. 393099 (JORF z 25. apríla 2021), ktorým sa zrušilo predchádzajúce znenie tohto ustanovenia, ktoré zahŕňalo povinnosť uchovávať osobné údaje „na účely vyšetrovania, odhaľovania a stíhania trestných činov alebo porušenia povinnosti vymedzenej v článku L. 336-3 [CPI]“ výlučne s cieľom umožniť v prípade potreby ich poskytnutie okrem iných úradu Hadopi. Svojím rozhodnutím č. 2021-976-977 QPC z 25. februára 2022 (Habib A. a iní) Conseil constitutionnel (Ústavná rada, Francúzsko) vyhlásila toto predchádzajúce znenie článku L. 34-1 CPCE za protiústavné, a to najmä z dôvodu, že „sporné ustanovenia tým, že umožňujú všeobecné a nediferencované uchovávanie údajov o pripojení, neprimerane zasahujú do práva na rešpektovanie súkromného života“ (bod 13). Tento súd totiž konštatoval, že údaje o pripojení, ktoré sa majú uchovávať na základe týchto ustanovení, sa týkajú nielen identifikácie používateľov elektronických komunikačných služieb, ale aj iných údajov, ktoré „vzhľadom na ich povahu, ich rôznorodosť a operácie spracúvania, ktorým môžu podliehať…, poskytujú o týchto používateľoch a prípadne tretích osobách početné a presné informácie, ktoré obzvlášť zasahujú do ich súkromného života“ (bod 11).

1° na účely trestného konania, predchádzania hrozbám pre verejnú bezpečnosť a ochrany národnej bezpečnosti informácie týkajúce sa totožnosti používateľa, a to až do uplynutia piatich rokov od skončenia platnosti jeho zmluvy;

2° na tie isté účely, ako sú uvedené v bode 1 tohto odseku IIa, ďalšie informácie poskytnuté používateľom pri uzatvorení zmluvy alebo vytvorení účtu, ako aj informácie týkajúce sa platby, a to až do uplynutia jedného roka od skončenia platnosti jeho zmluvy alebo zrušenia jeho účtu;

3° na účely boja proti trestnej činnosti a závažnej kriminalite, predchádzania závažným hrozbám pre verejnú bezpečnosť a ochrany národnej bezpečnosti, technické údaje umožňujúce identifikovať zdroj pripojenia alebo údaje týkajúce sa použitých koncových zariadení, a to až do uplynutia jedného roka od okamihu pripojenia alebo použitia koncových zariadení."

III. Konanie na Súdnom dvore

25. V odpovedi na výzvu adresovanú dotknutým osobám uvedeným v článku 23 Štatútu Súdneho dvora Európskej únie žalobcovia vo veci samej, francúzska, dánska, estónska, írska, holandská, fínska a švédska vláda, ako aj Európska komisia odpovedali na písomné otázky položené Súdnym dvorom.

26. Tí istí účastníci konania s výnimkou fínskej vlády, česká, španielska, cyperská, lotyšská a nórska vláda, ako aj EDPB a ENISA sa zúčastnili na pojednávaní, ktoré sa konalo 15. mája 2023.

IV. Analýza

27. Na základe mojej analýzy prejudiciálnych otázok v mojich prvých návrhoch som navrhol, aby Súdny dvor rozhodol, že článok 15 ods. 1 smernice 2002/58 sa má vykladať v tom zmysle, že nebráni vnútroštátnej právnej úprave, ktorá umožňuje poskytovateľom elektronických komunikačných služieb uchovávať a správnemu orgánu, akým je Hadopi[6], prístup k údajom obmedzeným na údaje o totožnosti zodpovedajúce IP adresám, aby tento orgán mohol identifikovať držiteľov týchto adries podozrivých zo zodpovednosti za porušovanie autorského práva a s ním súvisiacich práv, a prípadne voči nim prijať opatrenia bez toho, aby tento prístup podliehal predchádzajúcemu preskúmaniu zo strany súdu alebo nezávislého správneho orgánu, ak tieto údaje predstavujú jediný prostriedok vyšetrovania umožňujúci identifikáciu osoby, ktorej bola táto adresa pridelená v čase, keď došlo k porušeniu.

28. V týchto návrhoch sa budem snažiť detailnejšie rozobrať niektoré prvky mojej predchádzajúcej analýzy a otázky, o ktorých sa diskutovalo na pojednávaní 15. mája 2023, aby som vysvetlil dôvody, pre ktoré trvám tak na svojom návrhu odpovede na prejudiciálne otázky, ako aj na odôvodnení, ktoré k nemu viedlo.[7]

[6] Dňa 1. januára 2022 sa Conseil supérieur de l'audiovisuel (Najvyššia audiovizuálna rada) a Hadopi stali Autorité de régulation de la communication audiovisuelle et numérique (Úrad pre reguláciu audiovizuálnych a digitálnych komunikácií) (Arcom). Vzhľadom na obdobie, počas ktorého nastali skutkové okolnosti sporu vo veci samej, budem však v týchto návrhoch odkazovať na Hadopi.

[7] V tejto súvislosti tiež trvám na svojom návrhu preformulovať prejudiciálne otázky, ako aj na mojom chápaní ich predmetu. Hoci sa totiž v znení prejudiciálnych otázok uvádza len prístup k údajom o totožnosti zodpovedajúcim IP adresám, otázka prístupu k týmto údajom je neoddeliteľná od otázky ich uchovávania poskytovateľmi elektronických komunikačných služieb, takže analýza zlučiteľnosti uchovávania s právom Únie je nevyhnutným predpokladom analýzy zlučiteľnosti prístupu. V tejto súvislosti pozri bod 45 a nasl. mojich prvých návrhov. Rovnako, hoci sa prejudiciálne otázky týkajú „údajov o totožnosti zodpovedajúcich IP adrese", treba ich chápať tak, že sa týkajú aj prístupu k IP adresám umožňujúcim identifikovať zdroj pripojenia. V tejto súvislosti pozri bod 41 a nasl. mojich prvých návrhov.

29. Konkrétne preukážem, že umožnenie uchovávania údajov o totožnosti, ktoré zodpovedajú IP adresám, a prístupu k týmto údajom bez predchádzajúceho preskúmania na účely identifikácie páchateľov trestného činu, ak tieto údaje predstavujú jediný spôsob ich identifikácie, spĺňa požiadavky stanovené Súdnym dvorom v súvislosti s preskúmaním opatrení prijatých na základe článku 15 ods. 1 smernice 2002/58 (časť B).

30. Ďalej poukážem na to, že takéto riešenie nepredstavuje prehodnotenie prísnej judikatúry na ochranu základných práv rozvinutej Súdnym dvorom od rozsudkov Tele2 Sverige a Watson a i. [8] a La Quadrature du Net a i. [9], ale skôr jej nevyhnutný vývoj, ktorý podľa môjho názoru nadväzuje na zásady stanovené Súdnym dvorom. Toto rozlíšenie nie je len sémantické. Cieľom riešenia, ktoré navrhujem, totiž nie je spochybniť existujúcu judikatúru, ale v mene určitého pragmatizmu umožniť jej prispôsobenie za osobitných a veľmi úzko vymedzených okolností (časť C).

31. V záujme jasnosti a vzhľadom na to, že diskusie na pojednávaní ukázali potrebu spresnení v tomto ohľade, začnem svoju analýzu pripomenutím fungovania mechanizmu odstupňovanej reakcie zo strany Hadopi (časť A).

A. Mechanizmus odstupňovanej reakcie zo strany úradu Hadopi

32. Hadopi je nezávislý správny orgán zodpovedný za ochranu autorských práv a s nimi súvisiacich práv pred porušovaním týchto práv, ku ktorému dochádza na internete. Na tento účel bol zavedený tzv. mechanizmus „odstupňovanej reakcie“, ktorého vykonávanie je zverené komisii na ochranu práv úradu Hadopi.

33. Na túto komisiu sa obracajú s podnetmi organizácie nositeľov práv, v rámci ktorých určití prísažní zamestnanci poverení ministrom kultúry zhromažďujú na sieťach so vzájomným sprístupňovaním (*peer-to-peer*) IP adresy používateľov internetu, ktorí sprístupňujú verejnosti diela bez súhlasu ich majiteľov. Následne sa vyhotovia zápisnice. Tie obsahujú najmä IP adresu prístupu na internet použitú na páchanie týchto porušení autorského práva, dátum a čas zisteného porušenia, ako aj názov dotknutého diela, a sú postúpené komisii na ochranu práv úradu Hadopi. V tejto súvislosti treba zdôrazniť, ako uviedol EDPB, že spracúvanie osobných údajov zamestnancami organizácií držiteľov práv podlieha povoleniu zo strany Commission nationale de l'informatique et des libertés (Národná komisia pre informačné technológie a slobody) (CNIL), francúzskeho dozorného orgánu v oblasti ochrany údajov. [10]

34. Po prijatí zápisníc a po automatizovanej kontrole, ktorá má zabezpečiť, aby obsahovali všetky požadované údaje, môže komisia na ochranu práv úradu Hadopi získať od poskytovateľov elektronických komunikačných služieb totožnosť, poštovú adresu, elektronickú adresu a telefónne číslo majiteľa pripojenia, ktoré sa použilo na porušovanie autorského práva.

35. Hadopi tak môže tejto osobe zaslať „odporúčanie“, v ktorom ju informuje, že jej prístup na internet bol použitý v rozpore s autorskými právami, a ktorým vyzve osobu podozrivú z toho, že si nesplnila svoju povinnosť obozretnosti, pokiaľ ide o rešpektovanie diel chránených autorským právom alebo s ním súvisiacim právom na internete, aby túto povinnosť dodržiavala. Inak

[8] Rozsudok z 21. decembra 2016 (C-203/15 a C-698/15, ďalej len „rozsudok Tele2“, EU:C:2016:970).

[9] Rozsudok zo 6. októbra 2020 (C-511/18, C-512/18 a C-520/18, ďalej len „rozsudok La Quadrature du Net a i.“, EU:C:2020:791).

[10] Pozri v tejto súvislosti uznesenie CNIL č. 2010-225 z 10. júna 2010, ktorým sa mení povolenie pre Société des auteurs, compositeurs et éditeurs de musique (Združenie hudobných skladateľov, autorov a vydavateľov, Francúzsko) (SACEM) na vykonávanie spracúvania osobných údajov s cieľom vyšetrovania a zisťovania deliktov porušovania práv spáchaných prostredníctvom sietí vzájomného sprístupňovania súborov známych ako „peer-to-peer“ (povolenie č. 1425421).

povedané, odporúčanie je určené držiteľovi prístupu na internet, ktorý môže byť v skutočnosti inou osobou, než je osoba, ktorá dielo sprístupnila v rozpore s autorským právom. Druhé odporúčanie možno vydať v prípade druhého zistenia porušovania práv prostredníctvom toho istého prístupu na internet. V prípade ďalšieho opakovania môže komisia na ochranu práv úradu Hadopi rozhodnúť o postúpení veci prokurátorovi na účely trestného stíhania. V tejto súvislosti, ako spresnila francúzska vláda vo svojich prvých pripomienkach, zamestnanci Hadopi zodpovední za mechanizmus odstupňovanej reakcie sú prísažní zamestnanci poverení predsedom úradu Hadopi, sú viazaní služobným tajomstvom a sú jediní v rámci úradu Hadopi, ktorí majú povolenie na prístup k osobným údajom spracúvaným v rámci tohto mechanizmu.

36. V tejto súvislosti musím spresniť, že sa nezbierajú a úradu Hadopi neprenášajú údaje o všetkých používateľoch sietí vzájomného sprístupňovania, ktorí sa obmedzujú na sťahovanie takéhoto obsahu,[11] ale len údaje o osobách, ktoré sprístupnili obsah porušujúci práva, t. j. ktorí takýto obsah *nahrali*.

37. Na ilustráciu, v roku 2021 Hadopi dostal od organizácií nositeľov práv takmer štyri milióny zápisníc, poslal 210 595 prvých odporúčaní a 53 564 druhých odporúčaní a v 1 484 prípadoch sa obrátil na prokurátora republiky.

38. Po týchto pripomenutiach ukážem, prečo takýto mechanizmus, ktorý predpokladá uchovávanie a prístup k údajom o totožnosti zodpovedajúcim IP adresám, podľa môjho názoru spĺňa požiadavky judikatúry týkajúcej sa vnútroštátnych opatrení prijatých na základe článku 15 ods. 1 smernice 2002/58.

B. Dodržiavanie požiadaviek vyplývajúcich z judikatúry Súdneho dvora týkajúcej sa výkladu článku 15 ods. 1 smernice 2002/58

39. Keďže som už vo svojich prvých návrhoch pripomenul judikatúru Súdneho dvora týkajúcu sa uchovávania IP adries pridelených zdroju pripojenia a prístupu k nim,[12] v týchto návrhoch sa zameriam na to, čo podľa môjho názoru predstavuje jadro tejto judikatúry, a tým je na jednej strane požiadavka proporcionality a na druhej strane, pokiaľ ide o prístup k týmto údajom, možná potreba predchádzajúceho preskúmania zo strany súdu alebo nezávislého správneho orgánu.

1. O proporcionalite predmetného opatrenia

40. Na účely určenia zlučiteľnosti opatrenia na uchovávanie alebo prístup k údajom o totožnosti zodpovedajúcim IP adrese s právom Únie treba, ako opakovane zdôrazňuje Súdny dvor, pristúpiť k zosúladeniu rôznych legitímnych záujmov a dotknutých práv, ktorými sú jednak právo na ochranu súkromia a právo na ochranu osobných údajov[13] zaručené článkami 7 a 8 Charty, a jednak ochrana práv a slobôd iných a práv zakotvených v článkoch 3, 4, 6 a 7 Charty.[14] Chcem

[11] V súvislosti s fungovaním sietí so vzájomným sprístupňovaním a rôznych profiloch používateľov internetu na týchto sieťach pozri návrhy, ktoré som predniesol vo veci M.I.C.M. (C-597/19, EU:C:2020:1063, bod 37 a nasl.).

[12] Bod 53 a nasl. mojich prvých návrhov.

[13] Práva na ochranu súkromia a na ochranu osobných údajov sa v kontexte smernice 2002/58 odrážajú v zásadách dôvernosti správ a zákazu uchovávania s nimi súvisiacich údajov, ktoré sú v nej stanovené.

[14] Rozsudky La Quadrature du Net a i. (body 120 až 122, ako aj 127 a 128); z 5. apríla 2022, Commissioner of An Garda Síochána a i. (C-140/20, ďalej len „rozsudok Commissioner of An Garda Síochána a i.“, EU:C:2022:258, body 48 a 50), ako aj z 20. septembra 2022, SpaceNet a Telekom Deutschland (C-793/19 a C-794/19, ďalej len „rozsudok SpaceNet a Telekom Deutschland“, EU:C:2022:702, body 63 a 65).

dodať, že v prejednávanej veci musia byť práva na ochranu súkromia a na ochranu osobných údajov tiež zosúladené s vlastníckym právom zakotveným v článku 17 Charty, keďže mechanizmus odstupňovanej reakcie sa *in fine* týka ochrany autorského práva a s ním súvisiacich práv.

41. Súdny dvor v tejto súvislosti spresňuje, že toto zosúladenie, ktoré sa uskutočňuje na základe článku 15 ods. 1 smernice 2002/58, umožňuje členským štátom prijať opatrenie odchyľujúce sa od zásady dôvernosti, ak je takéto opatrenie „*nevyhnutné, vhodné a primerané* v demokratickej spoločnosti“ (kurzívou zvýraznil generálny advokát). Odôvodnenie 11 tejto smernice spresňuje, že opatrenie takejto povahy musí byť „prísne“ *proporcionálne* vo vzťahu k zamýšľanému účelu. [15]

42. Súdny dvor navyše v celom svojom odôvodnení týkajúcom sa výkladu článku 15 ods. 1 smernice 2002/58 odkazuje na zásadu proporcionality, a teda z nej robí kľúčový prvok preskúmania vnútroštátneho opatrenia na uchovávanie osobných údajov alebo prístup k nim, ktoré bolo prijaté na základe tohto ustanovenia.

43. Z podrobnejšieho výkladu tohto odôvodnenia vyplýva, že zásada proporcionality zahŕňa v kontexte článku 15 ods. 1 smernice 2002/58 rôzne aspekty týkajúce sa na jednej strane závažnosti zásahu do základných práv, ktorý zahŕňa uchovávanie údajov o prenose dát alebo prístup k týmto údajom, a na druhej strane nevyhnutnosti predmetného opatrenia.

44. Pokiaľ ide o uchovávanie údajov o totožnosti zodpovedajúcich IP adresám a prístup k týmto údajom zo strany úradu Hadopi, zastávam názor, že tak závažnosť zásahu, ako aj nevyhnutnosť týchto údajov by mali viesť Súdny dvor k tomu, aby prispôsobil svoje preskúmanie proporcionality vnútroštátneho opatrenia prijatého na základe článku 15 ods. 1 smernice 2002/58.

a) Relatívna závažnosť zásahu do základných práv

45. Z ustálenej judikatúry Súdneho dvora jasne vyplýva, že v súlade so zásadou proporcionality musí byť dôležitosť cieľa sledovaného opatrením prijatým podľa článku 15 ods. 1 smernice 2002/58 priamo úmerná závažnosti zásahu, ktorý z neho vyplýva. [16]

46. Súdny dvor konkrétne rozhodol, ako som zdôraznil vo svojich prvých návrhoch, že závažný zásah v oblasti prevencie, vyšetrovania, odhaľovania a stíhania trestných činov možno odôvodniť iba cieľom boja proti trestnej činnosti, ktorá musí byť tiež kvalifikovaná ako „závažná“. [17]

47. Pokiaľ ide o IP adresy, Súdny dvor uvádza, že hoci sú menej citlivé ako ostatné údaje o prenose dát, ich uchovávanie a analýza stále predstavujú závažné zásahy do základných práv, keďže ich možno použiť na vystopovanie kompletného prechádzania stránok používateľom internetu a v dôsledku toho na vytvorenie podrobného profilu tohto používateľa a vyvodenie presných záverov o jeho súkromnom živote. [18]

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

[16] Rozsudky Commissioner of An Garda Síochána a i. (bod 56) a SpaceNet a Telekom Deutschland (bod 71).

[17] Rozsudky Tele2 (bod 115); z 2. októbra 2018, Ministerio Fiscal (C-207/16, EU:C:2018:788, bod 56), a z 2. marca 2021, Prokuratuur (Podmienky prístupu k údajom týkajúcim sa elektronických komunikácií) (C-746/18, ďalej len „rozsudok Prokuratuur“, EU:C:2021:152, bod 33). Pozri tiež bod 92 mojich prvých návrhov.

[18] Pozri rozsudky La Quadrature du Net a i. (body 152 a 153), Commissioner of An Garda Síochána a i. (bod 73) a SpaceNet a Telekom Deutschland (bod 103). Pozri tiež body 63, 64 a 93 mojich prvých návrhov.

48. Vo veci samej je cieľom uchovávania a prístupu k údajom o totožnosti zodpovedajúcim IP adresám boj proti porušovaniu autorského práva a s ním súvisiacich práv. Podľa môjho názoru je pritom jasné, že tento boj nemôže spadať do boja proti závažnej trestnej činnosti,[19] aj keď je objem týchto porušení obrovský. Existuje teda nesúlad medzi závažnosťou zásahu do základných práv, ktorý zahŕňa predmetné opatrenie, a cieľom, ktorý sleduje.

49. Vo svojich prvých návrhoch som v súlade s judikatúrou Súdneho dvora zastával názor, že prístup úradu Hadopi k údajom o totožnosti zodpovedajúcim IP adrese skutočne predstavuje závažný zásah do základných práv. Ak som tiež dospel k záveru, že uchovávanie týchto údajov a prístup k nim by napriek tomu mali byť v prejednávanej veci povolené, musím po pojednávaní ešte uviesť niekoľko spresnení.

50. Mechanizmus odstupňovanej reakcie umožňuje úradu Hadopi na základe oznámenia organizácií nositeľov práv spojiť IP adresu osôb podozrivých z toho, že použili svoj prístup na internet na porušovanie autorského práva na sieťach vzájomného sprístupňovania, s totožnosťou tejto osoby, ako aj s výpisom zo súboru nahraného v rozpore s autorským právom. Ako uviedli Komisia a EDPB na pojednávaní, hoci takéto prvky určite umožňujú získať viac informácií ako len totožnosť údajného pôvodcu porušenia, nevedú k vyvodeniu veľmi presných záverov o súkromnom živote tejto osoby. Ako som totiž uviedol vo svojich prvých návrhoch,[20] ide len o odhalenie jednorazového prehliadania určitého obsahu, ktoré samo osebe neumožňuje stanoviť podrobný profil osoby, ktorá tak urobila.

51. Platí to o to viac, že v prvom rade veľká väčšina IP adries oznámených úradu Hadopi sú takzvané „dynamické“ IP adresy, ktoré sú svojou povahou premenlivé a zodpovedajú konkrétnej identite len v jednom okamihu, ktorý sa zhoduje so sprístupnením dotknutého obsahu. Vylučujú teda akékoľvek kompletné sledovanie.

52. Ďalej musím zdôrazniť, že ochrana základných práv na internete podľa mňa nemôže odôvodniť nemožnosť získať prístup výlučne k údajom týkajúcim sa IP adresy, obsahu diela a totožnosti osoby, ktorá ho sprístupnila v rozpore s autorskými právami, ale len to, že s uchovávaním týchto údajov a prístupom k nim musia byť spojené určité záruky. V tejto súvislosti sa mi zdá výstižná analógia s reálnym svetom: osoba podozrivá zo spáchania krádeže sa nemôže dovolávať svojho práva na ochranu súkromia, aby sa osoby zodpovedné za stíhanie tohto trestného činu mohli oboznámiť s ukradnutým obsahom. Naproti tomu sa táto osoba môže oprávnene dovolávať svojich základných práv, aby sa v priebehu konania zabránilo prístupu k súboru údajov, ktoré presahujú údaje potrebné na kvalifikáciu údajného trestného činu.

53. Napokon chcem uviesť, že na rozdiel od toho, čo tvrdia žalobkyne, mechanizmus odstupňovanej reakcie podľa všetkého nezahŕňa všeobecné monitorovanie používateľov sietí so vzájomným sprístupňovaním. Nejde totiž o preverovanie celej ich činnosti na danej sieti s cieľom určiť, či sprístupnili dielo v rozpore s autorskými právami, ale skôr o to, aby sa na základe súboru identifikovaného ako porušovanie práv určil držiteľ prístupu na internet, z ktorého používateľ internetu vykonal sprístupnenie. Rovnako, ako zdôraznil EDPB na pojednávaní, nejde o dohľad nad činnosťou všetkých používateľov sietí so vzájomným sprístupňovaním, ale len o dohľad nad

[19] Vo svojich prvých návrhoch som tvrdil, že pojem „závažná trestná činnosť“ treba vykladať autonómne, aby sa zabránilo akémukoľvek obchádzaniu požiadaviek stanovených v článku 15 ods. 1 smernice 2002/58 zo strany členských štátov. Na tomto stanovisku trvám. Musím však zdôrazniť, že aj keby Súdny dvor rozhodol, že definícia pojmu „závažná trestná činnosť“ je ponechaná na členské štáty, mala by byť v každom prípade stanovená v medziach práva Únie a nemohla by byť rozšírená do takej miery, že by zbavila toto ustanovenie jeho podstaty.

[20] Bod 101 mojich prvých návrhov.

činnosťou osôb, ktoré nahrávajú súbory porušujúce práva, pričom nahrávanie týchto súborov o to menej odhaľuje informácie týkajúce sa súkromného života osoby, že sa uskutočňuje len preto, aby títo používatelia internetu mohli následne sťahovať iné súbory.

54. Za týchto podmienok sa dôvody, ktoré viedli Súdny dvor k tomu, že považoval uchovávanie IP adries a prístup k nim za závažný zásah do základných práv, podľa môjho názoru neuplatnia, pokiaľ ide o taký mechanizmus odstupňovanej reakcie, aký uplatňuje Hadopi. Z toho vyplýva, že závažnosť zásahu, ktorý toto uchovávanie a prístup predpokladajú, by mala byť pri preskúmaní zásady proporcionality prispôsobená.

55. Inými slovami zastávam názor, že judikatúru Súdneho dvora týkajúcu sa závažnosti zásahu do základných práv spôsobeného uchovávaním IP adries a prístupom k nim treba vykladať tak, že neznamená, že tento zásah je vždy závažným zásahom, ale že je to tak len vtedy, keď IP adresy môžu viesť k vystopovaniu kompletného prechádzania stránok používateľom internetu a k vyvodeniu veľmi presných záverov o jeho súkromnom živote.

56. Keďže v takej situácii, o akú ide vo veci samej, to tak nie je, vyplýva z toho, že zásah, ktorý zahŕňa uchovávanie a prístup k údajom o totožnosti zodpovedajúcim IP adrese použitej na sprístupnenie obsahu v rozpore s autorským právom, by malo byť možné odôvodniť cieľom boja proti širšej trestnej činnosti, než je len závažná trestná činnosť.

57. Okrem toho chcem spresniť, že zásah do základných práv, ktorý predpokladá uchovávanie a prístup k údajom o totožnosti zodpovedajúcim IP adrese v situácii, o akú ide vo veci samej, nie je zhoršený okolnosťou, že držiteľ prístupu na internet používaného na sprístupnenie obsahu porušujúceho práva nie je nevyhnutne pôvodcom tohto sprístupnenia, takže odporúčanie zaslané úradom Hadopi by mohlo odhaliť tomuto držiteľovi uvedený obsah, ku ktorému mohla mať prístup tretia osoba. Na jednej strane pripomínam, že porušením, ktoré vyšetruje Hadopi, je nesplnenie povinnosti zabezpečiť, aby sa prístup nevyužíval na účely sprístupňovania obsahu v rozpore s autorským právom. Je preto potrebné, aby informácie umožňujúce jeho kvalifikáciu boli poskytnuté predpokladanému pôvodcovi sprístupnenia. Na druhej strane, ako som už uviedol, zastávam názor, že informácie týkajúce sa dotknutého diela neumožňujú vyvodiť presné závery o súkromnom živote osoby, ktorá je pôvodcom sprístupnenia. Prípadné poskytnutie týchto informácií majiteľovi internetového pripojenia teda nejde nad rámec toho, čo je nevyhnutné na umožnenie stíhania daného porušovania autorského práva.

b) Nevyhnutnosť predmetných údajov na odhaľovanie a stíhanie trestného činu

58. Na zabezpečenie proporcionality opatrenia na uchovávanie a prístup k údajom o prenose dát, akými sú údaje o totožnosti zodpovedajúce IP adrese, prijatého na základe článku 15 ods. 1 smernice 2002/58, je podľa judikatúry Súdneho dvora potrebné, aby bol zásah, ktorý toto opatrenie zahŕňa, obmedzený na to, čo je striktne nevyhnutné na dosiahnutie sledovaného cieľa. [21] Zdá sa mi, že tak je to práve v prípade opatrenia, o ktoré ide vo veci samej.

59. Ako som zdôraznil vo svojich prvých návrhoch, [22] zo samotnej judikatúry Súdneho dvora vyplýva, že v prípade trestného činu spáchaného výlučne online, ako je napríklad porušenie autorského práva na sieti so vzájomným sprístupňovaním, môže IP adresa predstavovať jediný

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

[22] Bod 78 mojich prvých návrhov.

prostriedok vyšetrovania umožňujúci identifikáciu osoby, ktorej bola táto adresa pridelená v čase spáchania trestného činu.[23] Z toho podľa môjho názoru vyplýva, že uchovávanie a prístup k údajom o totožnosti zodpovedajúcim IP adresám na účely odhaľovania a stíhania porušení autorských práv spáchaných online sú v súlade s judikatúrou striktne nevyhnutné na dosiahnutie sledovaného cieľa.

60. Je pravda, že akákoľvek požiadavka ochrany osobných údajov predpokladá obmedzenie vyšetrovacích právomocí. Vyplýva to zo samotnej zásady zosúladenia protichodných záujmov a takýto výsledok nemožno ako taký spochybniť. V prípade, že IP adresa predstavuje jediný prostriedok identifikácie osoby podozrivej z toho, že sa dopustila porušenia práva duševného vlastníctva online, sa však takáto situácia odlišuje od väčšiny trestných stíhaní, v súvislosti s ktorými Súdny dvor uvádza, že „účinnosť… nezávisí od jediného vyšetrovacieho nástroja, ale od všetkých vyšetrovacích nástrojov, ktorými na tento účel disponujú príslušné vnútroštátne orgány“[24]. Ak by sa pripustilo, že údaje o totožnosti zodpovedajúce IP adresám by nemali byť predmetom uchovávania a prístupu v takej situácii, o akú ide vo veci samej, neviedlo by to, ako každé opatrenie zabezpečujúce ochranu údajov o prenose dát, len k obmedzeniu vyšetrovacích právomocí, ale vnútroštátne orgány by to pripravilo aj o jediný prostriedok na odhaľovanie a stíhanie určitých trestných činov.

61. Inak povedané, podľa výkladu článku 15 ods. 1 smernice 2002/58, ktorý navrhujem, nejde o to, aby sa prostredníctvom preskúmania nevyhnutnosti takéhoto opatrenia umožnilo uchovávanie a prístup k údajom, ktoré iba *uľahčujú* odhaľovanie a stíhanie trestných činov, ak tieto trestné činy možno tiež odhaľovať a stíhať konkurenčnými prostriedkami, hoci aj menej účinnými. Naopak, ide o umožnenie uchovávania týchto údajov a prístupu k nim, ak sú *nevyhnutné* na identifikáciu osoby podozrivej zo spáchania trestného činu, ktorá bez týchto prostriedkov nemôže byť stíhaná, keďže predmetné údaje predstavujú jediný nástroj identifikácie používateľa internetu, pokiaľ k trestnému činu dochádza výlučne online.

62. Pokiaľ sa nepripustí, že celý rad trestných činov nemožno nikdy stíhať, mal by podľa mňa platiť takýto výklad.[25]

63. Z uvedeného vyplýva, že podľa môjho názoru vnútroštátna právna úprava umožňujúca poskytovateľom elektronických komunikačných služieb uchovávanie a správnemu orgánu prístup, ktoré sú obmedzené na údaje o totožnosti zodpovedajúce IP adresám, je v plnej miere primeraná sledovanému cieľu, konkrétne stíhaniu porušení autorského práva a s ním súvisiacich práv na internete, pokiaľ má zásah do základných práv, ktorý z nich vyplýva, obmedzenú závažnosť a pokiaľ tieto údaje predstavujú jediný prostriedok vyšetrovania umožňujúci identifikáciu osoby, ktorej bola táto adresa pridelená v čase, keď došlo k porušeniu.

64. Zastávam preto názor, že článok 15 ods. 1 smernice 2002/58 sa má vykladať v tom zmysle, že takejto právnej úprave nebráni.

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

[24] Rozsudok Commissioner of An Garda Síochána a i. (bod 69).

[25] Bod 81 mojich prvých návrhov. Pozri v tejto súvislosti tiež bod 79 a nasl. nižšie.

2. O existencii vhodných hmotnoprávnych a procesných záruk

65. Pokiaľ ide konkrétne o prístup k údajom o totožnosti zodpovedajúcim IP adresám, z judikatúry Súdneho dvora vyplýva, že samotná striktná proporcionalita opatrenia nestačí na to, aby bolo zlučiteľné s článkom 15 ods. 1 smernice 2002/58.

66. S cieľom zabezpečiť, aby bol prístup k údajom o prenose dát a polohe obmedzený na to, čo je striktne nevyhnutné, totiž Súdny dvor rozhodol, že je nevyhnutné, aby tento prístup podliehal predchádzajúcemu preskúmaniu zo strany súdu alebo nezávislého správneho orgánu, ktorý disponuje všetkými právomocami a poskytuje všetky záruky potrebné na zosúladenie rôznych dotknutých legitímnych záujmov a práv. [26]

67. Striktný výklad judikatúry by teda viedol ku konštatovaniu, že prístup úradu Hadopi k údajom o totožnosti zodpovedajúcim IP adresám osôb podozrivých z toho, že sa dopustili porušovania autorského práva na internete, by mal podliehať takémuto predchádzajúcemu preskúmaniu, ktoré v mechanizme odstupňovanej reakcie chýba.

68. Ako však tvrdila írska vláda na pojednávaní a ako som uviedol vo svojich prvých návrhoch, zastávam názor, že požiadavka predchádzajúceho preskúmania súdom alebo nezávislým správnym orgánom nie je systematickou požiadavkou, ale závisí od komplexnejšej analýzy dotknutého opatrenia, pričom sa zohľadní tak závažnosť zásahu, ktorý zahŕňa, ako aj záruky, ktoré stanovuje.

69. Chcem zdôrazniť, že v každom z rozsudkov, ktoré uvádzali túto požiadavku predchádzajúceho preskúmania súdom alebo nezávislým správnym orgánom, totiž išlo o vnútroštátne predpisy, ktoré umožňovali prístup ku všetkým údajom o prenose dát a polohe používateľov týkajúcich sa všetkých prostriedkov elektronickej komunikácie [27] alebo prinajmenšom pevnej a mobilnej telefónnej siete [28] identifikovaných používateľov.

70. Z toho vyvodzujem, že požiadavka takéhoto predchádzajúceho preskúmania sa riadi závažnosťou zásahu, o ktorý ide v dotknutých veciach. Ako zdôraznil Súdny dvor, išlo o údaje, ktoré „skutočne umožňuj[ú] vyvodiť presné, dokonca veľmi presné, závery týkajúce sa súkromného života osôb…, ako sú ich každodenné zvyklosti, miesta ich trvalého alebo prechodného pobytu, denné alebo iné presuny, vykonávané činnosti, spoločenské vzťahy týchto osôb a spoločenské kruhy, v ktorých sa pohybujú“ [29]. Navyše cieľom boli údaje o osobách, ktoré už boli identifikované a podozrivé zo spáchania trestného činu na základe iných indícií, pričom dotknuté údaje teda umožňovali posilniť usvedčujúce dôkazy proti dotknutému používateľovi rozšírením oblasti údajov, ktoré sa ho týkali.

71. Pokiaľ však ide o právnu úpravu, o ktorú ide vo veci samej, a ako som už zdôraznil, závažnosť zásahu, ktorý zahŕňa prepojenie údaja o totožnosti a IP adresy, je oveľa menšia ako závažnosť vyplývajúca z prístupu ku všetkým údajom o prenose dát a polohe osoby, keďže toto prepojenie neprináša nijaký dôkaz, ktorý by umožňoval vyvodiť presné závery o súkromnom živote dotknutej osoby.

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

[27] Rozsudky Tele2 a Commissioner of An Garda Síochána a i.

[28] Rozsudok Prokuratuur.

[29] Rozsudok Prokuratuur (bod 36).

72. Okrem toho, ako som uviedol vo svojich prvých návrhoch,[30] tieto údaje sa týkajú len osôb, ktoré sa po objektívnom konštatovaní používania IP adresy v rozpore s autorským právom, ktoré vydali organizácie nositeľov práv, dopustili konania, ktoré môže predstavovať nesplnenie povinnosti obozretnosti stanovenej v článku L.336-3 CPI. Tieto osoby nie sú vopred identifikované inými prostriedkami, keďže prepojenie IP adresy s údajmi o totožnosti je jediným prostriedkom identifikácie dotknutej osoby. Prístup k týmto údajom teda neumožňuje, ako to bolo vo veciach, o ktorých Súdny dvor predtým rozhodoval, získať dodatočné a presné informácie o činnosti osôb, ktoré už boli podozrivé na základe iných skutočností, ale len využiť IP adresu, ktorá je inak bezvýznamná. Za týchto podmienok sú údaje, ku ktorým má Hadopi prístup, *de facto* obmedzené.

73. Podľa môjho názoru existuje zásadný rozdiel medzi prístupom k osobným údajom týkajúcim sa osoby podozrivej zo spáchania trestného činu s cieľom preukázať jej vinu a odhalením totožnosti páchateľa už zisteného trestného činu.

74. Platí to podľa mňa o to viac, že zber IP adries na sieťach so vzájomným sprístupňovaním podlieha predchádzajúcemu povoleniu obmedzenému len na tieto údaje, takže Hadopi nikdy nedisponuje neobmedzeným súborom údajov, pokiaľ ide o používateľov internetu, u ktorých existuje podozrenie, že sa dopustili porušenia autorských práv na internete.[31]

75. Logika, na ktorej je založená požiadavka predchádzajúceho preskúmania súdom alebo nezávislým správnym orgánom, sa preto neuplatní v prípade takého mechanizmu odstupňovanej reakcie, o aký ide vo veci samej, takže takáto požiadavka sa mi nezdá byť potrebná na to, aby sa zabezpečilo, že zásah do základných práv vyplývajúci z tohto mechanizmu je obmedzený na to, čo je striktne nevyhnutné.

76. Z uvedeného vyplýva, že vnútroštátna právna úprava umožňujúca uchovávanie údajov o totožnosti zodpovedajúcich IP adresám a prístup k týmto údajom zo strany nezávislého správneho orgánu, akým je Hadopi, s cieľom identifikovať držiteľov týchto adries podozrivých zo zodpovednosti za porušovania autorských práv, bez toho, aby tento prístup podliehal predchádzajúcemu preskúmaniu zo strany súdu alebo nezávislého správneho orgánu, v konečnom dôsledku rešpektuje zásady stanovené judikatúrou Súdneho dvora, ak tieto údaje predstavujú jediný prostriedok identifikácie osoby, ktorej bola IP adresa pridelená v čase, keď došlo k porušeniu, takže článok 15 ods. 1 smernice 2002/58 sa má vykladať v tom zmysle, že takejto právnej úprave nebráni.

77. Okrem týchto úvah, ktoré sa týkajú veci samej, musím ešte uviesť všeobecnejšie poznámky o potrebe rozvíjať judikatúru Súdneho dvora týmto smerom.

C. Potrebný a ohraničený vývoj judikatúry

78. Viaceré tvrdenia svedčia v prospech spresnenia judikatúry Súdneho dvora týkajúcej sa uchovávania a prístupu k údajom, akými sú IP adresy spojené s údajmi o totožnosti.

[30] Bod 102 mojich prvých návrhov.

[31] Bod 33 vyššie.

79. V prvom rade, ako som už zdôraznil,[32] v situácii, o akú ide vo veci samej, je získanie údajov o totožnosti zodpovedajúcich IP adrese jediným prostriedkom vyšetrovania umožňujúcim identifikáciu osoby, ktorej bola táto adresa pridelená v čase, keď došlo k dotknutému porušeniu.

80. Z toho nevyhnutne vyplýva, že ak by Súdny dvor dospel k záveru, že článok 15 ods. 1 smernice 2002/58 predsa len bráni ich uchovávaniu a prístupu k nim, vnútroštátne orgány by *de facto* prišli o jediný prostriedok identifikácie a pôvodcovia dotknutého porušenia by tak nemohli byť nikdy stíhaní.[33] To ma vo svojich prvých návrhoch viedlo k tomu, aby som spomenul možnosť systémovej beztrestnosti tohto porušenia.[34]

81. Riziko systémovej beztrestnosti sa neobmedzuje len na porušovanie autorského práva na sieťach so vzájomným sprístupňovaním, ale sa vzťahuje, ako uviedla česká vláda na pojednávaní, na všetky trestné činy, ku ktorým dochádza výlučne online.

82. Trestné činy, ktorých páchatelia môžu byť identifikovaní len prostredníctvom ich IP adries, by totiž nemohli byť nikdy stíhaní a ustanovenia, ktoré ich sankcionujú, by sa nikdy nemohli uplatniť, ak by sa rozhodlo, že tak uchovávanie údajov, ako aj prístup k nim sú v rozpore s právom Únie.

83. V tejto súvislosti chcem uviesť, že je pravda, ako uviedli žalobkyne vo veci samej, že iné prostriedky by teoreticky mohli umožniť identifikáciu páchateľov niektorých trestných činov spáchaných výlučne online. Odkazujú tak najmä na identifikátor používaný na sociálnych sieťach a údaje súvisiace s účtom používateľa, ako je jeho emailová adresa, telefónne číslo alebo prvok týkajúci sa jej súkromného života, ktoré táto osoba odhalila. Na to, aby sa takéto údaje spojili s totožnosťou osoby, je však potrebné dôkladné vyšetrovanie, počas ktorého sa skúma online aktivita používateľa internetu. Zdá sa mi teda, že použitie takýchto prostriedkov vyšetrovania umožňuje, na rozdiel od samotnej IP adresy, vyvodiť veľmi presné závery o súkromnom živote osôb, takže uchovávanie týchto údajov a prístup k nim by v tomto zmysle boli v rozpore s článkom 15 ods. 1 smernice 2002/58.

84. Za týchto podmienok prístup k údajom o totožnosti zodpovedajúcim IP adrese používateľa internetu určite nie je jediným teoretickým prostriedkom vyšetrovania umožňujúcim identifikovať osobu, ktorá bola držiteľom tejto adresy v čase spáchania trestného činu, avšak je jediným, ktorý umožňuje jej stíhanie a zároveň zahŕňa najmenší zásah do základných práv týchto osôb, a v dôsledku toho zabraňuje všeobecnej beztrestnosti.

85. V druhom rade opäť zdôrazňujem, že takéto riešenie by podľa môjho názoru umožnilo zosúladiť dve línie judikatúry Súdneho dvora, zdroje určitého napätia, ktoré som identifikoval vo svojich prvých návrhoch[35] a v návrhoch, ktoré som predniesol vo veci M.I.C.M.[36], konkrétne na jednej strane judikatúru týkajúcu sa uchovávania údajov a prístupu k nim a na druhej strane judikatúru týkajúcu sa poskytovania IP adries pridelených zdroju pripojenia v rámci žalôb na ochranu práv duševného vlastníctva podaných súkromnými osobami.

86. V treťom rade hoci treba judikatúru Súdneho dvora od rozsudkov Tele2 a La Quadrature du Net a i. privítať v tom zmysle, že umožnila zavedenie rámca na ochranu základných práv používateľov elektronických komunikačných služieb, je predsa len poznačená určitou

[32] Bod 59 vyššie.

[33] Bod 62 vyššie.

[34] Bod 78 a nasl. mojich prvých návrhov.

[35] Bod 69 a nasl. mojich prvých návrhov.

[36] C-597/19, EU:C:2020:1063.

kazuistikou. Súdny dvor vo veciach, ktoré prejednával, totiž postupne spresňoval svoju judikatúru, čo mu umožnilo preskúmať rôzne vnútroštátne právne úpravy z hľadiska článku 15 ods. 1 smernice 2002/58. Súdny dvor však nemôže prakticky predvídať všetky opatrenia, ktoré by mohli byť predmetom analýzy z hľadiska tohto ustanovenia. Svedčí o tom aj počet návrhov na začatie prejudiciálneho konania [37] podaných na Súdny dvor po vydaní rozsudku Tele2, čo podľa môjho názoru potvrdzuje ťažkosti, s ktorými sa môžu potýkať vnútroštátne súdy pri uplatňovaní zásad uvedených v judikatúre Súdneho dvora na situácie odlišné od tých, ktoré viedli k dotknutým rozsudkom. [38]

87. Z toho teda vyplýva, že určitá pružnosť sa mi zdá nevyhnutná, ak sa Súdnemu dvoru predkladajú na preskúmanie opatrenia, ktoré nebolo možné predpokladať v predchádzajúcich rozsudkoch, ako sú napríklad právne úpravy týkajúce sa trestných činov, ktoré možno stíhať len vtedy, ak sú údaje o totožnosti zodpovedajúce IP adresám uchovávané a prístupné, čím sa doteraz Súdny dvor nemusel nikdy zaoberať.

88. Nejde teda, ako tvrdila dánska vláda, o prehodnotenie judikatúry Súdneho dvora, ale o to, aby sa pripustilo, že na základe zásad, z ktorých vychádza, možno za veľmi obmedzených okolností dosiahnuť vyváženejšie riešenie.

89. Výklad článku 15 ods. 1 smernice 2002/58, ktorý navrhujem, totiž umožňuje uchovávanie údajov o totožnosti zodpovedajúcich IP adresám a prístup k týmto údajom, len pokiaľ ide o stíhanie trestných činov, ktorých páchatelia by bez týchto údajov nemohli byť identifikovaní. Týka sa teda iba trestných činov, ku ktorým dochádza výlučne online, a nespochybňuje riešenia uvádzané v judikatúre v súvislosti s uchovávaním širších údajov a prístupom k nim, ktoré sledujú odlišné ciele.

V. Návrh

90. Vzhľadom na všetky predchádzajúce úvahy navrhujem, aby Súdny dvor odpovedal na prejudiciálne otázky, ktoré predložila Conseil d'État (Štátna rada, Francúzsko), takto:

Článok 15 ods. 1 smernice Európskeho parlamentu a Rady 2002/58/ES z 12. júla 2002, týkajúcej sa spracovávania osobných údajov a ochrany súkromia v sektore elektronických komunikácií (smernica o súkromí a elektronických komunikáciách), zmenenej smernicou Európskeho parlamentu a Rady 2009/136/ES z 25. novembra 2009, v spojení s článkami 7, 8, 11 a článkom 52 ods. 1 Charty základných práv Európskej únie

[37] Rozsudky z 2. októbra 2018, Ministerio Fiscal (C-207/16, EU:C:2018:788); La Quadrature du Net a i.; Prokuratuur; Commissioner of An Garda Síochána a i., ako aj SpaceNet a Telekom Deutschland.

[38] V tejto súvislosti môže nárast návrhov na začatie prejudiciálneho konania, ktoré sa týkajú výkladu článku 15 ods. 1 smernice 2002/58, naznačovať aj určitú formu neochoty vnútroštátnych súdov uplatňovať zásady stanovené Súdnym dvorom na mierne odlišné situácie, a to z dôvodu osobitostí vnútroštátnych právnych systémov. Pozri v tejto súvislosti najmä CAMERON, I.: Metadata retention and national security: *Privacy international* and *La Quadrature du Net*. In: *Common Market Law Review*. 2021, roč. 58, č. 5, s. 1433 – 1471, alebo aj BERTRAND, B.: L'audace sans le tact: jusqu'où la Cour de justice peut-elle aller trop loin? In: *Dalloz IP/IT*. 2021, č. 9, s. 468 – 472. V záujme zachovania plodného dialógu medzi Súdnym dvorom a súdmi členských štátov sa mi preto zdá o to dôležitejšie, aby Súdny dvor mohol preukázať prispôsobenie, ak si to okolnosti vyžadujú. Ako uviedli autori právnej vedy, vysoký štandard ochrany stanovený judikatúrou Súdneho dvora nemôže byť skutočne účinný bez podpory vnútroštátnych súdov, ktoré sú primárne zodpovedné za jeho uplatňovanie. Pozri v tejto súvislosti najmä TEYSSEDRE, J.: Strictly regulated retention and access regimes for metadata: *Commissioner of An Garda Siochana*. In: *Common Market Law Review*. 2023, roč. 60, č. 2, s. 569 – 588, a SIRINELLI, J.: La protection des données de connexion par la Cour de justice: cartographie d'une jurisprudence européenne inédite. In: *Revue trimestrielle de droit européen*. 2021, roč. 57, č. 2, s. 313 – 329.

sa má vykladať v tom zmysle, že:

nebráni vnútroštátnej právnej úprave, ktorá umožňuje poskytovateľom elektronických komunikačných služieb uchovávať a správnemu orgánu zodpovednému za ochranu autorského práva a s ním súvisiacich práv pred porušovaním týchto práv na internete získať prístup k údajom obmedzeným na údaje o totožnosti zodpovedajúce IP adresám, aby tento orgán mohol identifikovať držiteľov týchto adries podozrivých zo zodpovednosti za toto porušovanie a prípadne voči nim prijať opatrenia bez toho, aby tento prístup podliehal predchádzajúcemu preskúmaniu zo strany súdu alebo nezávislého správneho orgánu, ak tieto údaje predstavujú jediný prostriedok vyšetrovania umožňujúci identifikáciu osôb, ktorým boli uvedené adresy pridelené v čase, keď došlo k porušeniu.