



Zbierka súdnych rozhodnutí

ROZSUDOK SÚDNEHO DVORA (veľká komora)

z 20. septembra 2022*

[Znenie opravené uznesením z 27. októbra 2022]

„Návrh na začatie prejudiciálneho konania – Spracovávanie osobných údajov v sektore elektronických komunikácií – Dôvernosť správy – Poskytovatelia elektronických komunikačných služieb – Všeobecné a nediferencované uchovávanie údajov o prenose dát a polohe – Smernica 2002/58/ES – Článok 15 ods. 1 – Charta základných práv Európskej únie – Články 6, 7, 8 a 11, ako aj článok 52 ods. 1 – Článok 4 ods. 2 ZEÚ“

V spojených veciach C-793/19 a C-794/19,

ktorých predmetom sú návrhy na začatie prejudiciálneho konania podľa článku 267 ZFEÚ, podané rozhodnutiami Bundesverwaltungsgericht (Spolkový správny súd, Nemecko) z 25. septembra 2019 a doručené Súdnemu dvoru 29. októbra 2019, ktoré súvisia s konaniami:

Bundesrepublik Deutschland, zastúpená Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen,

proti

SpaceNet AG (C-793/19),

Telekom Deutschland GmbH (C-794/19),

SÚDNY DVOR (veľká komora),

v zložení: predseda K. Lenaerts, predsedovia komôr A. Arabadžiev, A. Prechal, S. Rodin, I. Jarukaitis a I. Ziemele, sudcovia T. von Danwitz, M. Safjan, F. Biltgen, P. G. Xuereb (spravodajca), N. Piçarra, L. S. Rossi a A. Kumin,

generálny advokát: M. Campos Sánchez-Bordona,

tajomník: D. Dittert, vedúci oddelenia,

so zreteľom na písomnú časť konania a po pojednávaní z 13. septembra 2021,

* Jazyk konania: nemčina.

so zreteľom na pripomienky, ktoré predložili:

- Bundesrepublik Deutschland, zastúpená Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen, v zastúpení: C. Mögelin, splnomocnený zástupca,
- [Opravené uznesením z 27. októbra 2022] SpaceNet AG, v zastúpení: M. Bäcker, Universitätsprofessor,
- Telekom Deutschland GmbH, v zastúpení: T. Mayen, Rechtsanwalt,
- nemecká vláda, v zastúpení: J. Möller, F. Halibi, M. Hellmann, D. Klebs, a E. Lankenau, splnomocnení zástupcovia,
- dánska vláda, v zastúpení: M. Jespersen, J. Nymann-Lindgren, V. Pasternak Jørgensen a M. Søndahl Wolff, splnomocnení zástupcovia,
- estónska vláda, v zastúpení: A. Kalbus a M. Kriisa, splnomocnené zástupkyne,
- Írsko, v zastúpení: A. Joyce a J. Quaney, splnomocnení zástupcovia, za právnej pomoci D. Fennelly, BL, a P. Gallagher, SC,
- španielska vláda, v zastúpení: L. Aguilera Ruiz, splnomocnený zástupca,
- francúzska vláda, v zastúpení: A. Daniel, D. Dubois, J. Illouz, E. de Moustier a T. Stéhelin, splnomocnení zástupcovia,
- cyperská vláda, v zastúpení: I. Neophytou, splnomocnená zástupkyňa,
- holandská vláda, v zastúpení: M. K. Bulterman, A. Hanje a C. S. Schillemans, splnomocnené zástupkyne,
- poľská vláda, v zastúpení: B. Majczyna, D. Lutostańska a J. Sawicka, splnomocnení zástupcovia,
- fínska vláda, v zastúpení: A. Laine a M. Pere, splnomocnení zástupcovia,
- švédská vláda, v zastúpení: H. Eklinder, A. Falk, J. Lundberg, C. Meyer-Seitz, R. Shahsavan Eriksson a H. Shev, splnomocnené zástupkyne,
- Európska komisia, v zastúpení: G. Braun, S. L. Kaléda, H. Kranenborg, M. Wasmeier a F. Wilman, splnomocnení zástupcovia,
- Európsky dozorný úradník pre ochranu údajov, v zastúpení: A. Buchta, D. Nardi, N. Stolič a K. Ujazdowski, splnomocnení zástupcovia,

po vypočutí návrhov generálneho advokáta na pojednávaní 18. novembra 2021,

vyhlásil tento

Rozsudok

- 1 Návrhy na začatie prejudiciálneho konania sa týkajú výkladu článku 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) (Ú. v. ES L 201, 2002, s. 37; Mim. vyd. 13/029, s. 514), zmenenej 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“), v spojení s článkami 6 až 8 a 11, ako aj s článkom 52 ods. 1 Charty základných práv Európskej únie (ďalej len „Charta“) a článkom 4 ods. 2 ZEÚ.
- 2 Tieto návrhy boli podané v rámci sporov medzi Bundesrepublik Deutschland (Spolková republika Nemecko), zastúpenou Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (Spolková agentúra pre elektrickú energiu, plyn, telekomunikácie, poštu a železnice, Nemecko), a spoločnosťami SpaceNet AG (vec C-793/19) a Telekom Deutschland GmbH (vec C-794/19) vo veci povinnosti uloženej týmto spoločnostiam uchovávať údaje o prenose dát a polohe týkajúce sa telekomunikácií ich zákazníkov.

Právny rámec

Právo Únie

Smernica 95/46/ES

- 3 Smernica Európskeho parlamentu a Rady 95/46/ES z 24. októbra 1995 o ochrane fyzických osôb pri spracovaní osobných údajov a voľnom pohybe týchto údajov (Ú. v. ES L 281, 1995, s. 31; Mim. vyd. 13/015, s. 355) bola s účinnosťou od 25. mája 2018 zrušená nariadením Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46 (všeobecné nariadenie o ochrane údajov) (Ú. v. EÚ L 119, 2016, s. 1).
- 4 Článok 3 ods. 2 smernice 95/46 stanovoval:

„Táto smernica sa neuplatňuje na spracovanie osobných údajov:

- v priebehu činností, ktoré sú mimo rozsahu zákona [práva – *neoficiálny preklad*] spoločenstva, ako sú tie, ktoré sú uvedené v hlave V a VI Zmluvy o Európskej únii, a v žiadnom prípade sa neuplatňuj[e] na operácie spracovania týkajúce sa verejnej bezpečnosti, obrany, bezpečnosti štátu (vrátane hospodárskej prosperity štátu, keď sa operácia spracovania týka záležitostí bezpečnosti štátu) a činností štátu v oblastiach trestného zákona [práva – *neoficiálny preklad*],
- fyzickou osobou v priebehu osobnej činnosti, alebo činnosti týkajúcej sa domácnosti [fyzickou osobou na výkon výlučne osobných alebo domácich činností – *neoficiálny preklad*].“

Smernica 2002/58

5 Odôvodnenia 2, 6, 7 a 11 smernice 2002/58 stanovujú:

„(2) Táto smernica sa snaží rešpektovať základné práva a dodržiavať princípy uznané najmä [Chartou]. Táto smernica sa snaží najmä o plné zabezpečenie práv stanovených v článkoch 7 a 8 [tejto 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 uchovávanía a spracovávanía údajov týkajúcich sa účastníkov a užívateľov.

...

(11) Podobne ako smernica [95/46] 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 [podpísaného 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.“

6 Článok 1 tejto smernice s názvom „Rozsah platnosti a cieľ“ stanovuje:

„1. Touto smernicou sa ustanovuje harmonizácia vnútroštátnych ustanovení požadovaných na zabezpečenie primeranej úrovne ochrany základných práv a slobôd, a najmä práva na súkromie a dôvernosť, z hľadiska spracovávanía osobných údajov v elektronickom komunikačnom sektore a zabezpečenia voľného pohybu takých údajov a elektronických komunikačných zariadení a služieb v spoločenstve.

2. Ustanovenia tejto smernice spodrobňujú a dopĺňajú smernicu [95/46] na účely uvedené v odseku 1. Okrem toho poskytujú ochranu legitímnych záujmov účastníkov, ktorí sú právnickými osobami.

3. Táto smernica sa nevzťahuje na činnosti, ktoré sú mimo pôsobnosti [Zmluvy o FEÚ], ako sú činnosti podľa hlavy V a VI Zmluvy [EÚ] a v žiadnom prípade na činnosti týkajúce sa verejnej bezpečnosti, obrany, bezpečnosti štátu (vrátane ekonomického blahobytu štátu, keď sa činnosti týkajú záležitostí bezpečnosti štátu) a činnosti [činnosti štátu – *neoficiálny preklad*] v oblasti trestného práva.“

7 Podľa článku 2 uvedenej smernice s názvom „Definície“:

„Pokiaľ nie je stanovené inak, platia definície v smernici [95/46] a v smernici Európskeho parlamentu a Rady 2002/21/ES zo 7. marca 2002 o spoločnom regulačnom rámci pre elektronické komunikačné siete a služby (rámcová smernica) [(Ú. v. ES L 108, 2002, s. 33; Mim. vyd. 13/029, s. 349)].

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 spracované 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;

...“

8 Článok 3 smernice 2002/58, 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.“

9 Podľa článku 5 tejto smernice s názvom „Dôvernosť správy“:

„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 [počúvanie, odpočúvanie, uchovávanie – *neoficiálny preklad*] a iné druhy narušovania [odpočúvania – *neoficiálny preklad*] 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 vyžiadala, mohol tieto služby poskytnúť.“

10 Článok 6 smernice 2002/58 s názvom „Prevádzkové dáta [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.

3. Na účely marketingu elektronických komunikačných služieb alebo na poskytovanie služieb s pridanou hodnotou poskytovateľ verejnej dostupnej elektronickej komunikačnej služby môže spracúvať údaje uvedené v odseku 1 v rozsahu a počas trvania potrebného na také služby alebo marketing, ak účastník alebo užívateľ, ktorého sa údaje týkajú, dá na to predtým svoj súhlas. Užívatelia alebo účastníci musia mať možnosť kedykoľvek odvolať svoj súhlas na spracovanie údajov.

...

5. Spracovávanie prevádzkových dát [údajov o prenose dát – *neoficiálny preklad*], v súlade s odsekmi 1, 2, 3 a 4, sa musí obmedziť na osoby konajúce na pokyn poskytovateľa verejných komunikačných sietí a verejne dostupných elektronických komunikačných služieb, ktoré sú zodpovedné za faktúrovanie alebo riadenie prevádzky, vybavovanie dotazov zákazníkov, odhaľovanie podvodov, marketing elektronických komunikačných služieb alebo poskytovanie služieb s pridanou hodnotou a musí sa obmedziť na to, čo je nevyhnutné na účely takých činností.

...“

- 11 Článok 9 tejto smernice s názvom „Miestne dáta [Údaje o polohe – *neoficiálny preklad*] iné než prevádzkové dáta [údaje o prenose dát – *neoficiálny preklad*]“ v odseku 1 stanovuje:

„Ak sa môžu spracovávať miestne dáta [údaje o polohe – *neoficiálny preklad*] iné než prevádzkové dáta [údaje o prenose dát – *neoficiálny preklad*], ktoré sa týkajú užívateľov alebo účastníkov verejnej komunikačnej siete alebo verejne dostupných elektronických komunikačných služieb, také údaje sa môžu spracovávať, len keď sú anonymné alebo len so súhlasom užívateľov alebo účastníkov v rozsahu a trvaní nevyhnutnom na poskytovanie služby s pridanou hodnotou. Poskytovateľ služby musí informovať užívateľov alebo účastníkov predtým, než získa ich súhlas o druhu miestnych dát [údajov o polohe – *neoficiálny preklad*] iných, než sú prevádzkové dáta [údaje o prenose dát – *neoficiálny preklad*], ktoré bude spracovávať, o účele a dobe trvania spracovávania a o tom, či budú dáta prenášané tretej strane na účely poskytovania služby s pridanou hodnotou. ...“

- 12 Článok 15 smernice 2002/58, 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 spoločenstva vrátane tých, ktoré sú uvedené v článku 6 ods. 1 a 2 [ZEÚ].“

Nemecké právo

TKG

- 13 § 113a ods. 1 prvá veta Telekommunikationsgesetz (zákon o telekomunikáciách) z 22. júna 2004 (BGBl. 2004 I, s. 1190), v znení uplatniteľnom na spor vo veci samej (ďalej len „TKG“), znie:

„Povinnosti týkajúce sa uchovávania, používania a bezpečnosti údajov o prenose dát vymedzené v § 113b až §113g sa vzťahujú na poskytovateľov verejne dostupných telekomunikačných služieb koncovým užívateľom.“

- 14 Podľa § 113b TKG:

„1. Poskytovatelia uvedení v § 113a ods. 1 musia uchovávať údaje v tuzemsku takto:

(1) desať týždňov, ak ide o údaje uvedené v odsekoch 2 a 3,

(2) štyri týždne, ak ide o údaje o polohe uvedené v odseku 4.

2. Poskytovatelia verejne dostupných telefónnych služieb uchovávajú:

- (1) telefónne číslo alebo iný identifikačný znak volajúceho a volaného čísla a v prípade presmerovania alebo prepojenia hovoru každé ďalšie zúčastnené číslo;
- (2) dátum a čas začatia a skončenia spojenia s uvedením príslušného časového pásma;
- (3) informácie o využívanej službe, ak v rámci telefónnej služby možno využívať rôzne druhy služieb;
- (4) v prípade mobilných telefónnych služieb tiež
 - a) medzinárodný identifikačný kód mobilného účastníka v prípade volajúceho a volaného čísla;
 - b) medzinárodný identifikačný kód volajúceho a volaného koncového zariadenia;
 - c) dátum a čas prvej aktivácie služby s uvedením príslušného časového pásma v prípade predplatených služieb;
- (5) v prípade internetových telefónnych služieb aj IP adresy volajúceho a volaného čísla a pridelené užívateľské mená.

Prvý pododsek sa primerane uplatní

- (1) v prípade komunikácie prostredníctvom krátkej textovej, multimedialnej alebo podobnej správy; v tomto prípade sa údaje uvedené v prvom pododseku bode 2 nahradzujú okamihom odoslania a prijatia správy;
- (2) na neprijaté hovory alebo hovory, ktoré boli neúspešné z dôvodu zásahu prevádzkovateľa sústavy...

3. Poskytovatelia verejne dostupných služieb prístupu k internetu uchovávajú:

- (1) IP adresu pridelenú účastníkovi na používanie internetu;
- (2) jednoznačnú identifikáciu čísla umožňujúceho prístup k internetu, ako aj pridelené užívateľské meno;
- (3) dátum a čas začiatku a konca používania internetu z pridenej IP adresy s uvedením príslušného časového pásma.

4. V prípade použitia mobilných telefónnych služieb sa musí uchovávať označenie buniek, ktoré sa v prípade volajúceho a volaného čísla použili na začiatku spojenia. Pokiaľ ide o verejne dostupné služby prístupu k internetu, v prípade mobilného spojenia sa musí uchovávať označenie buniek, ktoré sa použili na začiatku internetového spojenia. Tiež sa musia uchovávať údaje, z ktorých vyplýva zemepisná poloha a maximálny dosah antén, ktoré využíva príslušná bunka.

5. Na základe tohto ustanovenia sa nemôže uchovávať obsah komunikácie, údaje o navštívených internetových stránkach a údaje o službách elektronickej pošty.

6. Na základe tohto ustanovenia sa nemôžu uchovávať údaje, na ktorých sú založené spojenia uvedené v § 99 ods. 2 To platí primerane pre telefónne spojenia, v prípade ktorých sú volajúcimi účastníkmi subjekty uvedené v § 99 ods. 2 Primerane sa uplatní § 99 ods. 2 druhá až siedma veta.

...“

15 Spojeniami uvedenými v § 99 ods. 2 TKG, na ktoré odkazuje § 113b ods. 6 TKG, sú spojenia s osobami, orgánmi a organizáciami sociálnej alebo náboženskej povahy, ktoré poskytujú výlučne alebo hlavne volajúcim, ktorí zostávajú v zásade v anonymite, telefonickú pomoc v prípadoch psychickej alebo sociálnej núdze a na ktoré sa vzťahujú alebo na ktorých pracovníkov sa v tejto súvislosti vzťahujú osobitné povinnosti zachovávanie dôvernosti. Výnimka stanovená v § 99 ods. 2 druhej a štvrtej vete TKG je podmienená zápisom volaných účastníkov na ich žiadosť do zoznamu, ktorý vypracovala Spolková agentúra pre elektrickú energiu, plyn, telekomunikácie, poštu a železnice, po tom, čo držitelia telefónnych čísel potvrdia povahu poskytovaných služieb predložením osvedčenia vydaného verejnoprávnym orgánom, inštitúciou, subjektom alebo nadáciou.

16 Podľa § 113c ods. 1 a 2 TKG:

„1. Údaje uchovávané podľa § 113b sa môžu:

- (1) poskytnúť orgánu činnému v trestnom konaní, ak požiada o ich poskytnutie s odvolaním sa na zákonné ustanovenie, ktoré ho oprávňuje získavať údaje uvedené v § 113b na účely stíhania mimoriadne závažných trestných činov;
- (2) poskytnúť bezpečnostnému orgánu spolkových krajín, ak požiada o ich poskytnutie s odvolaním sa na zákonné ustanovenie, ktoré ho oprávňuje získavať údaje uvedené v § 113b na účely odvrátenia konkrétnej hrozby pre zdravie, život alebo slobodu osoby alebo pre existenciu spolkového štátu alebo spolkovej krajiny;

...

2. Nositelia povinností uvedených v § 113a ods. 1 nemôžu používať údaje uchovávané podľa § 113b na iné účely než tie, ktoré sú uvedené v odseku 1.“

17 § 113d TKG stanovuje:

„Nositeľ povinností uvedenej v § 113a ods. 1 musí zabezpečiť, aby údaje uchovávané na základe povinnosti uchovávanie podľa § 113b ods. 1 boli chránené technickými a organizačnými opatreniami zodpovedajúcimi stavu techniky proti neoprávnenej kontrole a použitiu. Tieto opatrenia zahŕňajú najmä:

- (1) použitie mimoriadne bezpečného postupu šifrovania;
- (2) uchovávanie v samostatných úložiskách, ktoré sú oddelené od úložísk určených na bežné prevádzkové úlohy;
- (3) uchovávanie s vysokou úrovňou ochrany pred kybernetickými útokmi v systémoch na spracúvanie údajov, ktoré nie sú pripojené k internetu;

- (4) obmedzenie prístupu k zariadeniam na spracúvanie údajov na osoby, ktoré osobitne splnomocnil nositeľ povinnosti, a
- (5) povinná účasť aspoň dvoch osôb, ktoré na tento účel osobitne splnomocnil nositeľ povinnosti, na prístupe k údajom.“

18 § 113e TKG znie:

„1. Nositeľ povinnosti uvedenej v § 113a ods. 1 musí zabezpečiť, aby sa na účely kontroly ochrany údajov zaznamenal každý prístup a najmä načítanie, rozmnoženie, zmena, vymazanie a zablokovanie údajov uchovávaných na základe povinnosti uchovávať údaje podľa § 113b ods. 1. Zaznamená sa:

- (1) čas prístupu;
- (2) osoby, ktoré majú prístup k údajom;
- (3) účel a druh prístupu.

2. Zaznamenané údaje nemožno použiť na iné účely, než sú účely kontroly ochrany údajov.

3. Nositeľ povinnosti uvedenej v § 113a ods. 1 musí zabezpečiť, aby sa zaznamenané údaje po uplynutí jedného roka vymazali.“

19 Na zabezpečenie obzvlášť vysokej úrovne bezpečnosti a kvality údajov Spolková agentúra pre elektrickú energiu, plyn, telekomunikácie, poštu a železnice vypracúva súbor požiadaviek v súlade s § 113f ods. 1 TKG, ktoré sa musia v súlade s § 113f ods. 2 TKG priebežne vyhodnocovať a prípadne upravovať. § 113g TKG vyžaduje, aby osobitné bezpečnostné opatrenia boli zahrnuté do vyhlásenia o bezpečnostnej politike, ktoré má predložiť nositeľ povinnosti.

StPO

20 § 100g ods. 2 prvá veta Strafprozessordnung (Trestný poriadok, ďalej len „StPO“) znie:

„Ak určité skutočnosti odôvodňujú podozrenie, že niekto sa ako páchatel alebo spolupáchateľ dopustil jedného z obzvlášť závažných trestných činov uvedených v druhej vete alebo v prípadoch, v ktorých je pokus trestný, sa pokúsil spáchať taký trestný čin a tento trestný čin je v konkrétnom prípade tiež obzvlášť závažný, možno získať údaje o prenose dát uchovávané podľa § 113b [TKG], pokiaľ by prešetrenie skutkového stavu alebo zistenie miesta, v ktorom sa zdržiava obvinený, iným spôsobom bolo podstatne sťažené alebo nemožné a získanie týchto údajov je primerané významu veci.“

21 § 101a ods. 1 StPO stanovuje, že na získanie údajov o prenose dát podľa § 100g StPO je potrebné povolenie súdu. Podľa § 101a ods. 2 StPO musia odôvodnenia rozhodnutia obsahovať zásadné úvahy týkajúce sa nevyhnutnosti a primeranosti opatrenia v danom konkrétnom prípade. § 101a ods. 6 StPO stanovuje povinnosť informovať účastníkov dotknutej telekomunikácie.

Spory vo veciach samých a prejudiciálna otázka

- 22 SpaceNet a Telekom Deutschland poskytujú v Nemecku verejne dostupné služby prístupu k internetu. Druhá z nich okrem toho poskytuje v Nemecku aj verejne dostupné telefónne služby.
- 23 Títo poskytovatelia služieb napadli na Verwaltungsgericht Köln (Správny súd Kolín nad Rýnom, Nemecko) povinnosť uchovávať od 1. júla 2017 telekomunikačné údaje o prenose dát a polohe svojich zákazníkov, ktorú im ukladá § 113a ods. 1 v spojení s § 113b TKG.
- 24 Rozsudkami z 20. apríla 2018 Verwaltungsgericht Köln (Správny súd Kolín nad Rýnom) rozhodol, že SpaceNet a Telekom Deutschland nie sú povinné uchovávať údaje o prenose dát uvedené v § 113b ods. 3 TKG, ktoré sa týkajú telekomunikácií zákazníkov, ktorým poskytujú prístup k internetu, a že Telekom Deutschland nie je navyše povinná uchovávať údaje o prenose dát uvedené v § 113b ods. 2 prvej a druhej vete TKG, ktoré sa týkajú telekomunikácií zákazníkov, ktorým poskytuje prístup k verejne dostupným telefónnym službám. Tento súd totiž s prihliadnutím na rozsudok z 21. decembra 2016, Tele2 Sverige a Watson a i. (C-203/15 a C-698/15, EU:C:2016:970), konštatoval, že táto povinnosť uchovávania je v rozpore s právom Únie.
- 25 Spolková republika Nemecko podala proti týmto rozsudkom opravné prostriedky „Revision“ na Bundesverwaltungsgericht (Spolkový správny súd, Nemecko), ktorý podal návrh na začatie prejudiciálneho konania.
- 26 Tento súd sa domnieva, že otázka, či povinnosť uchovávania stanovená § 113a ods. 1 v spojení s § 113b TKG je v rozpore s právom Únie, závisí od výkladu smernice 2002/58.
- 27 V tejto súvislosti vnútroštátny súd uvádza, že Súdny dvor už v rozsudku z 21. decembra 2016, Tele2 Sverige a Watson a i. (C-203/15 a C-698/15, EU:C:2016:970), s konečnou platnosťou rozhodol, že právna úprava týkajúca sa uchovávania údajov o prenose dát a polohe, ako aj prístupu vnútroštátnych orgánov k týmto údajom v zásade patrí do pôsobnosti smernice 2002/58.
- 28 Uvádza tiež, že povinnosť uchovávania, o ktorú ide vo veci samej, môže byť odôvodnená len na základe článku 15 ods. 1 tejto smernice, keďže obmedzuje práva vyplývajúce z článku 5 ods. 1, článku 6 ods. 1 a z článku 9 ods. 1 smernice 2002/58.
- 29 V tejto súvislosti pripomína, že z rozsudku z 21. decembra 2016, Tele2 Sverige a Watson a i. (C-203/15 a C-698/15, EU:C:2016:970), vyplýva, že článok 15 ods. 1 smernice 2002/58 v spojení s článkami 7, 8 a 11, ako aj s článkom 52 ods. 1 Charty sa má vykladať v tom zmysle, že bráni vnútroštátnej právnej úprave, ktorá na účely boja proti trestnej činnosti stanovuje všeobecné a nediferencované uchovávanie všetkých údajov o prenose dát a polohe všetkých účastníkov a registrovaných užívateľov, ktoré sa týkajú všetkých prostriedkov elektronickej komunikácie.
- 30 Podľa vnútroštátneho súdu však vnútroštátna právna úprava, o ktorú ide vo veci samej, rovnako ako vnútroštátne právne úpravy dotknuté vo veciach, v ktorých bol vydaný uvedený rozsudok, nevyžaduje nijaký dôvod na uchovávanie údajov ani akúkoľvek súvislosť medzi uchovávanými údajmi a trestným činom alebo rizikom pre verejnú bezpečnosť. Táto vnútroštátna právna úprava totiž stanovuje bezdôvodné, všeobecné a osobne, časovo a miestne nediferencované uchovávanie veľkej časti relevantných telekomunikačných údajov o prenose dát.

- 31 Vnútroštátny súd sa však domnieva, že nie je vylúčené, že povinnosť uchovávania, o ktorú ide vo veci samej, môže byť odôvodnená podľa článku 15 ods. 1 smernice 2002/58.
- 32 V prvom rade uvádza, že na rozdiel od vnútroštátnych právnych úprav, o ktoré išlo vo veciach, v ktorých bol vydaný rozsudok z 21. decembra 2016, *Tele2 Sverige a Watson a i.* (C-203/15 a C-698/15, EU:C:2016:970), vnútroštátna právna úprava dotknutá vo veci samej nevyžaduje uchovávanie všetkých telekomunikačných údajov o prenose dát všetkých účastníkov a registrovaných užívateľov, ktoré sa týkajú všetkých prostriedkov elektronickej komunikácie. Ako vyplýva z § 113b ods. 5 a 6 TKG, nielenže obsah komunikácií je vylúčený z povinnosti uchovávania, ale tiež sa nesmú uchovávať údaje o navštívených internetových stránkach, údaje o službách elektronickej pošty a údaje o spojeniach sociálnej a náboženskej povahy na určité čísla alebo z nich.
- 33 V druhom rade tento súd uvádza, že § 113b ods. 1 TKG stanovuje dobu uchovávania v trvaní štyroch týždňov pre údaje o polohe a desať týždňov pre údaje o prenose dát, zatiaľ čo smernica Európskeho parlamentu a Rady 2006/24/ES z 15. marca 2006 o uchovávaní údajov vytvorených alebo spracovaných v súvislosti s poskytovaním verejne dostupných elektronických komunikačných služieb alebo verejných komunikačných sietí a o zmene a doplnení smernice 2002/58/ES (Ú. v. EÚ L 105, 2006, s. 54), z ktorej vychádzajú vnútroštátne právne predpisy dotknuté vo veciach, v ktorých bol vydaný rozsudok z 21. decembra 2016, *Tele2 Sverige a Watson a i.* (C-203/15 a C-698/15, EU:C:2016:970), stanovovala dobu uchovávania v rozmedzí od šiestich mesiacov do dvoch rokov.
- 34 Vnútroštátny súd sa pritom domnieva, že aj keď vylúčenie niektorých komunikačných prostriedkov alebo niektorých kategórií údajov a obmedzenie doby uchovávania nepostačujú na vylúčenie akéhokoľvek rizika vytvorenia úplného profilu dotknutých osôb, je toto riziko v rámci vykonávania vnútroštátnej právnej úpravy, o ktorú ide vo veci samej, prinajmenšom výrazne nižšie.
- 35 V treťom rade táto právna úprava obsahuje prísne obmedzenia, pokiaľ ide o ochranu uchovávaných údajov a prístup k nim. Na jednej strane tak zaručuje účinnú ochranu uchovávaných údajov pred rizikom zneužitia, ako aj pred akýmkoľvek neoprávneným prístupom k týmto údajom. Na druhej strane uchovávané údaje možno použiť len na účely boja proti závažným trestným činom alebo na účely odvrátenia hrozby pre zdravie, život alebo slobodu osoby alebo pre existenciu spolkového štátu alebo spolkovej krajiny.
- 36 Vo štvrtom rade výklad článku 15 ods. 1 smernice 2002/58 v zmysle všeobecnej nezlučiteľnosti akéhokoľvek bezdôvodného uchovávania údajov s právom Únie by mohol byť v rozpore s povinnosťou členských štátov konať, ktorá vyplýva z práva na bezpečnosť zakotveného v článku 6 Charty.
- 37 V piatom rade sa vnútroštátny súd domnieva, že výklad článku 15 smernice 2002/58 v tom zmysle, že bráni všeobecnému uchovávaniu údajov, by značne obmedzil rozhodovací priestor vnútroštátneho zákonodarcu v oblasti postihu trestných činov a verejnej bezpečnosti, ktorý v súlade s článkom 4 ods. 2 ZEÚ zostáva vo výlučnej zodpovednosti každého členského štátu.
- 38 V šiestom rade sa vnútroštátny súd domnieva, že je potrebné zohľadniť judikatúru Európskeho súdu pre ľudské práva (ďalej len „ESLP“) a uvádza, že ESLP rozhodol, že článok 8 Európskeho dohovoru o ochrane ľudských práv a základných slobôd (ďalej len „EDLP“) nebráni vnútroštátnym

ustanoveniam, ktoré stanovujú masívne zachytávanie cezhraničných tokov údajov s ohľadom na hrozby, ktorým v súčasnosti čelia mnohé štáty, a technologické nástroje, o ktoré sa v súčasnosti môžu opierať teroristi a zločinci pri dopúšťaní sa protiprávnych konaní.

- 39 Za týchto okolností Bundesverwaltungsgericht (Spolkový správny súd) rozhodol prerušiť konanie a položiť Súdnemu dvoru túto prejudiciálnu otázku:

„Má sa článok 15 smernice [2002/58] vzhľadom na články 7, 8 a 11, ako aj článok 52 ods. 1 [Charty] na jednej strane a článok 6 [uvedenej Charty] a tiež článok 4 [ZEÚ] na druhej strane vykladať v tom zmysle, že bráni vnútroštátnej právnej úprave, ktorá poskytovateľom verejne dostupných elektronických komunikačných služieb ukladá povinnosť uchovávať údaje o prenose dát a polohe konečných užívateľov týchto služieb, ak

- (1) táto povinnosť nezávisí od osobitného dôvodu, čo sa týka územného, časového alebo priestorového hľadiska;
- (2) sa povinnosť uchovávania v rámci poskytovania verejne dostupných telefónnych služieb, vrátane prenosu krátkych textových, multimediálnych alebo iných podobných správ, ako aj neprijatých alebo neúspešných hovorov, vzťahuje na tieto údaje:
 - a) telefónne číslo alebo iná identifikácia volajúceho a volaného čísla a v prípade presmerovania alebo prepojenia hovoru akékoľvek ďalšie zúčastnené číslo;
 - b) dátum a čas začatia a skončenia spojenia, resp. v prípade prenosu krátkych textových, multimediálnych alebo iných podobných správ, čas odoslania a prijatia správy s uvedením príslušného časového pásma;
 - c) informácie o využívaní služby, ak v rámci telefónnej služby možno využívať rôzne druhy služieb;
 - d) v prípade mobilných telefónnych služieb tiež
 - i) medzinárodný identifikačný kód mobilného účastníka v prípade volajúceho a volaného čísla;
 - ii) medzinárodný identifikačný kód volajúceho a volaného koncového zariadenia;
 - iii) dátum a čas prvej aktivácie služby s uvedením príslušného časového pásma v prípade predplatených služieb;
 - iv) označenie buniek, ktoré sa v prípade volajúceho a volaného čísla použili na začiatku spojenia;
 - e) v prípade internetových telefónnych služieb aj IP adresy volajúceho a volaného čísla a pridelené užívateľské mená;
- (3) sa povinnosť uchovávania v prípade poskytovania verejne dostupných služieb prístupu k internetu vzťahuje na tieto údaje:
 - a) IP adresa pridelená účastníkovi na používanie internetu;
 - b) jednoznačná identifikácia čísla umožňujúceho prístup k internetu, ako aj pridelené užívateľské meno;
 - c) dátum a čas začiatku a konca používania internetu z pridelení IP adresy s uvedením príslušného časového pásma;
 - d) v prípade mobilného spojenia označenie bunky, ktorá sa použila na začiatku internetového spojenia;
- (4) nemožno uchovávať tieto údaje:
 - a) obsah komunikácie;
 - b) údaje o navštívených internetových stránkach;

- c) údaje o službách elektronickej pošty;
 - d) údaje týkajúce sa spojení na určité čísla alebo z určitých čísel osôb, orgánov alebo organizácií pôsobiacich v sociálnej alebo náboženskej oblasti;
- (5) je doba uchovávaní v prípade údajov o polohe, t. j. pokiaľ ide o označenie použitej bunky, štyri týždne a v prípade ostatných údajov desať týždňov;
- (6) je zaručená účinná ochrana uchovávaných údajov pred rizikom ich zneužitia, ako aj pred akýmkoľvek neoprávneným prístupom a
- (7) uchovávané údaje možno použiť len na účely stíhania závažných trestných činov a odvrátenia konkrétnej hrozby pre zdravie, život alebo slobodu osoby alebo pre existenciu spolkového štátu alebo spolkovej krajiny okrem IP adresy pridelené účastníkovi na používanie internetu, ktorú možno použiť v rámci poskytnutia informácií o účastníkovi na účely stíhania akýchkoľvek trestných činov, odvrátenia nebezpečenstva pre verejnú bezpečnosť a verejný poriadok, ako aj na plnenie úloh spravodajských služieb?“

Konanie na Súdnom dvore

- 40 Rozhodnutím predsedu Súdneho dvora z 3. decembra 2019 boli veci C-793/19 a C-794/19 spojené na účely písomnej a ústnej časti konania, ako aj rozsudku.
- 41 Rozhodnutím predsedu Súdneho dvora zo 14. júla 2020 bolo konanie v spojených veciach C-793/19 a C-794/19 prerušené podľa článku 55 ods. 1 písm. b) Rokovacieho poriadku Súdneho dvora až do vyhlásenia rozsudku vo veci La Quadrature du Net a i. (C-511/18, C-512/18 a C-520/18).
- 42 Keďže Súdny dvor vydal 6. októbra 2020 rozsudok vo veci La Quadrature du Net a i. (C-511/18, C-512/18 a C-520/18, EU:C:2020:791), predseda Súdneho dvora 8. októbra 2020 nariadil pokračovanie v konaní v spojených veciach C-793/19 a C-794/19.
- 43 Vnútroštátny súd, ktorému kancelária Súdneho dvora oznámila tento rozsudok, uviedol, že trvá na svojom návrhu na začatie prejudiciálneho konania.
- 44 V tejto súvislosti tento vnútroštátny súd najprv poznamenal, že povinnosť uchovávaní stanovená právnou úpravou, o ktorú ide vo veci samej, sa týka nižšieho počtu údajov a kratšej doby uchovávaní, než stanovujú vnútroštátne právne predpisy dotknuté vo veciach, v ktorých bol vydaný rozsudok zo 6. októbra 2020, La Quadrature du Net a i. (C-511/18, C-512/18 a C-520/18, EU:C:2020:791). Tieto osobitosti obmedzujú možnosť, že uchovávané údaje môžu umožniť vyvodiť veľmi presné závery o súkromnom živote osôb, ktorých údaje boli uchovávané.
- 45 Následne znovu uviedol, že vnútroštátna právna úprava dotknutá vo veci samej zabezpečuje účinnú ochranu uchovávaných údajov pred rizikami zneužitia a neoprávneného prístupu.
- 46 Napokon zdôraznil, že pretrváva neistota, pokiaľ ide o otázku zlučiteľnosti uchovávaní IP adries, ktorú stanovuje vnútroštátna právna úprava dotknutá vo veci samej, s právom Únie, a to z dôvodu nesúladu medzi bodmi 155 a 168 rozsudku zo 6. októbra 2020, La Quadrature du Net a i. (C-511/18, C-512/18 a C-520/18, EU:C:2020:791). Podľa vnútroštátneho súdu tak z tohto rozsudku vyplýva neistota, pokiaľ ide o otázku, či Súdny dvor vyžaduje na uchovávanie IP adries

dôvod uchovávaní spojený s cieľom ochrany národnej bezpečnosti, boja proti závažnej trestnej činnosti alebo predchádzania vážnym hrozbám pre verejnú bezpečnosť, ako to vyplýva z bodu 168 uvedeného rozsudku, alebo či je uchovávanie IP adries povolené aj v prípade neexistencie konkrétneho dôvodu, pričom len použitie uchovávaných údajov je obmedzené uvedenými cieľmi, ako vyplýva z bodu 155 toho istého rozsudku.

O prejudiciálnej otázke

- 47 Svojou prejudiciálnou otázkou sa vnútroštátny súd v podstate pýta, či sa má článok 15 ods. 1 smernice 2002/58 v spojení s článkami 6 až 8 a 11, ako aj s článkom 52 ods. 1 Charty a článkom 4 ods. 2 ZEÚ vykladať v tom zmysle, že bráni vnútroštátnemu legislatívnemu opatreniu, ktoré s určitými výnimkami ukladá poskytovateľom verejne dostupných elektronických komunikačných služieb na účely uvedené v článku 15 ods. 1 tejto smernice, a najmä na účely stíhania závažných trestných činov alebo odvrátenia konkrétnej hrozby pre národnú bezpečnosť, všeobecné a nediferencované uchovávanie zásadných údajov o prenose dát a polohe koncových užívateľov týchto služieb, pričom stanovuje dobu uchovávaní v dĺžke niekoľkých týždňov a pravidiel, ktoré majú zabezpečiť účinnú ochranu uchovávaných údajov pred rizikami zneužitia, ako aj pred akýmkoľvek neoprávneným prístupom k týmto údajom.

O uplatniteľnosti smernice 2002/58

- 48 Pokiaľ ide o argumentáciu Írska, ako aj francúzskej, holandskej, poľskej a švédskej vlády, podľa ktorej vnútroštátna právna úprava dotknutá vo veci samej, keďže bola prijatá najmä na účely ochrany národnej bezpečnosti, nepatrí do pôsobnosti smernice 2002/58, stačí pripomenúť, že taká vnútroštátna právna úprava, o akú ide vo veci samej, ktorá poskytovateľom elektronických komunikačných služieb ukladá povinnosť uchovávať údaje o prenose dát a polohe najmä na účely ochrany národnej bezpečnosti a boja proti trestnej činnosti, patrí do pôsobnosti smernice 2002/58 (rozsudok zo 6. októbra 2020, *La Quadrature du Net a i.*, C-511/18, C-512/18 a C-520/18, EU:C:2020:791, bod 104).

O výklade článku 15 ods. 1 smernice 2002/58

Pripomenutie zásad vyplývajúcich z judikatúry Súdneho dvora

- 49 Z ustálenej judikatúry vyplýva, že na účely výkladu ustanovenia práva Únie treba zohľadniť nielen jeho znenie, ale aj jeho kontext a ciele sledované právnou úpravou, ktorej je súčasťou, a najmä vývoj tejto právnej úpravy (rozsudok z 5. apríla 2022, *Commissioner of An Garda Síochána a i.*, C-140/20, EU:C:2022:258, bod 32, ako aj citovaná judikatúra).
- 50 Zo samotného znenia článku 15 ods. 1 smernice 2002/58 vyplýva, že legislatívne opatrenia, ktoré táto smernica umožňuje členským štátom prijať za podmienok, ktoré stanovuje, sa môžu týkať len „obmedzenia rozsahu“ práv a povinností stanovených najmä v článkoch 5, 6 a 9 smernice 2002/58 (rozsudok z 5. apríla 2022, *Commissioner of An Garda Síochána i.*, C-140/20, EU:C:2022:258, bod 33).

- 51 Pokiaľ ide o systém zavedený touto smernicou, do ktorého patrí jej článok 15 ods. 1, treba pripomenúť, že podľa článku 5 ods. 1 prvej a druhej vety uvedenej smernice sú členské štáty povinné zabezpečiť prostredníctvom svojej vnútroštátnej právnej úpravy dôvernosť správ a príslušných údajov o prenose dát prenášaných pomocou verejnej komunikačnej siete a verejne dostupných elektronických komunikačných služieb. Majú povinnosť zakázať najmä počúvanie, odpočúvanie, uchovávanie a iné druhy odpočúvania alebo dohľadu nad správami a príslušnými údajmi o prenose dát zo strany iných osôb, než sú užívatelia, bez súhlasu príslušných užívateľov, pokiaľ to nie je zákonne oprávnené v súlade s článkom 15 ods. 1 tej istej smernice (rozsudok z 5. apríla 2022, Commissioner of An Garda Síochána i., C-140/20, EU:C:2022:258, bod 34).
- 52 V tejto súvislosti Súdny dvor už rozhodol, že článok 5 ods. 1 smernice 2002/58 zakotvuje zásadu dôvernosti elektronických komunikácií a príslušných údajov o prenose dát a okrem iného stanovuje, že sa akýmkoľvek iným osobám než užívateľom v zásade zakazuje bez súhlasu týchto užívateľov uchovávať tieto komunikácie a tieto údaje (rozsudky zo 6. októbra 2020, La Quadrature du Net a i., C-511/18, C-512/18 a C-520/18, EU:C:2020:791, bod 107, ako aj z 5. apríla 2022, Commissioner of An Garda Síochána a i., C-140/20, EU:C:2022:258, bod 35).
- 53 Toto ustanovenie odráža cieľ sledovaný normotvorcom Únie pri prijímaní smernice 2002/58. Z dôvodovej správy k návrhu smernice Európskeho parlamentu a Rady týkajúcej sa spracovávania osobných údajov a ochrany súkromia v sektore elektronických komunikácií [KOM(2000) 385 v konečnom znení], na základe ktorej bola prijatá smernica 2002/58, totiž vyplýva, že normotvorca Únie chcel „zabezpečiť, aby aj naďalej bola zaručená vysoká úroveň ochrany osobných údajov a súkromia pre všetky elektronické komunikačné služby, bez ohľadu na použité technológie“. Účelom uvedenej smernice, ako vyplýva najmä z jej odôvodnení 6 a 7, je chrániť užívateľov elektronických komunikačných služieb pred rizikami pre ich osobné údaje a súkromie, ktoré vyplývajú z nových technológií a predovšetkým zo zvyšovania kapacity automatického uchovávania a spracovávania údajov. Ako sa uvádza najmä v odôvodnení 2 tej istej smernice, zámerom normotvorcu Únie je zabezpečiť plné dodržiavanie práv stanovených v článku 7 Charty, ktorý sa týka ochrany súkromia, a článku 8 Charty, ktorý sa týka ochrany osobných údajov (pozri v tomto zmysle rozsudok z 5. apríla 2022, Commissioner of An Garda Síochána a i., C-140/20, EU:C:2022:258, bod 36, ako aj citovanú judikatúru).
- 54 Prijatím smernice 2002/58 tak normotvorca Únie konkretizoval tieto práva, takže užívatelia elektronických komunikačných prostriedkov majú v zásade právo očakávať, že ich komunikácia a s ňou súvisiace údaje zostanú anonymné a nebude možné ich zaznamenať bez ich súhlasu (rozsudky zo 6. októbra 2020, La Quadrature du Net a i., C-511/18, C-512/18 a C-520/18, EU:C:2020:791, bod 109, ako aj z 5. apríla 2022, Commissioner of An Garda Síochána a i., C-140/20, EU:C:2022:258, bod 37).
- 55 Pokiaľ ide o spracúvanie a uchovávanie údajov o prenose dát týkajúcich sa účastníkov a užívateľov poskytovateľmi elektronických komunikačných služieb, článok 6 smernice 2002/58 v odseku 1 stanovuje, že tieto údaje sa musia vymazať alebo anonymizovať, ak už naďalej nie sú potrebné na účely prenosu správy, a v odseku 2 spresňuje, že údaje o prenose dát potrebné na účely fakturácie účastníka a platby za spojenie sa môžu spracovávať iba do konca obdobia, počas ktorého môže byť faktúra právne napadnutá alebo sa môže uplatniť nárok na platbu. Pokiaľ ide o údaje o polohe iné ako údaje o prenose dát, článok 9 ods. 1 uvedenej smernice stanovuje, že tieto údaje sa môžu spracovávať len za určitých podmienok a po ich anonymizácii alebo po získaní súhlasu užívateľov alebo účastníkov.

- 56 Smernica 2002/58 sa teda neobmedzuje na ohraničenie prístupu k takýmto údajom prostredníctvom záruk určených na predchádzanie zneužívaniu, ale zakotvuje tiež najmä zásadu zákazu ich uchovávaní tretími osobami (rozsudok z 5. apríla 2022, Commissioner of An Garda Síochána a i., C-140/20, EU:C:2022:258, bod 39).
- 57 V rozsahu, v akom článok 15 ods. 1 smernice 2002/58 umožňuje členským štátom prijať legislatívne opatrenia na „obmedzenie rozsahu“ práv a povinností stanovených najmä v článkoch 5, 6 a 9 tejto smernice, ako sú práva a povinnosti vyplývajúce zo zásad dôvernosti správ a zákazu uchovávaní s nimi súvisiacich údajov, ktoré sú pripomenuté v bode 52 tohto rozsudku, toto ustanovenie stanovuje výnimku zo všeobecného pravidla stanoveného najmä v týchto článkoch 5, 6 a 9, a teda sa musí v súlade s ustálenou judikatúrou vykladať reštriktívne. Takéto ustanovenie teda nemôže odôvodniť, že výnimka zo zásadnej povinnosti zabezpečiť dôvernosť elektronických komunikácií a s ňou súvisiacich údajov, a najmä výnimka zo zákazu uchovávať tieto údaje stanovená v článku 5 uvedenej smernice, sa stane pravidlom, pretože inak by bolo toto ustanovenie z veľkej časti zbavené svojho rozsahu pôsobnosti (rozsudok z 5. apríla 2022, Commissioner of An Garda Síochána a i., C-140/20, EU:C:2022:258, bod 40, ako aj citovaná judikatúra).
- 58 Pokiaľ ide o ciele, ktoré môžu odôvodniť obmedzenie práv a povinností stanovených najmä v článkoch 5, 6 a 9 smernice 2002/58, Súdny dvor už rozhodol, že výpočet cieľov uvedených v článku 15 ods. 1 prvej vete tejto smernice je taxatívny, v dôsledku čoho musí legislatívne opatrenie prijaté na základe tohto ustanovenia skutočne a striktno zodpovedať jednému z týchto cieľov (rozsudok z 5. apríla 2022, Commissioner of An Garda Síochána a i., C-140/20, EU:C:2022:258, bod 41, ako aj citovaná judikatúra).
- 59 Okrem toho z článku 15 ods. 1 tretej vety smernice 2002/58 vyplýva, že opatrenia prijaté členskými štátmi podľa tohto ustanovenia musia rešpektovať všeobecné zásady práva Únie, medzi ktoré patrí zásada proporcionality, a zabezpečiť dodržiavanie základných práv zaručených Chartou. V tejto súvislosti Súdny dvor už rozhodol, že povinnosť uložená poskytovateľom elektronických komunikačných služieb zo strany členského štátu na základe vnútroštátnej právnej úpravy, podľa ktorej sú povinní uchovávať údaje o prenose dát na účely ich prípadného sprístupnenia príslušným vnútroštátnym orgánom, vyvoláva otázky týkajúce sa súladu nielen s článkami 7 a 8 Charty, ale aj s článkom 11 Charty týkajúcim sa slobody prejavu, pričom táto sloboda predstavuje jednu zo základných podstát demokratickej a pluralitnej spoločnosti a je súčasťou hodnôt, na ktorých je podľa článku 2 ZEÚ Európska únia založená (pozri v tomto zmysle rozsudok z 5. apríla 2022, Commissioner of An Garda Síochána a i., C-140/20, EU:C:2022:258, body 42 a 43, ako aj citovanú judikatúru).
- 60 V tejto súvislosti treba spresniť, že samotné uchovávanie údajov o prenose dát a polohe predstavuje samo osebe na jednej strane výnimku zo zákazu stanoveného v článku 5 ods. 1 smernice 2002/58, ktorým sa akejkolvek inej osobe, než sú užívatelia, zakazuje uchovávať tieto údaje, a na druhej strane zásah do základných práv na rešpektovanie súkromného života a ochranu osobných údajov, ktoré sú zakotvené v článkoch 7 a 8 Charty, bez ohľadu na to, či predmetné informácie týkajúce sa súkromného života majú alebo nemajú citlivú povahu alebo či pre dotknuté osoby z dôvodu tohto zásahu vplynuli alebo nevplynuli prípadné nepriaznivé následky, alebo či sa uchovávané údaje následne použijú alebo nie (rozsudok z 5. apríla 2022, Commissioner of An Garda Síochána a i., C-140/20, EU:C:2022:258, bod 44, ako aj citovaná judikatúra).

- 61 Tento záver sa javí o to dôvodnejší, že údaje o prenose dát a polohe môžu odhaliť informácie o značnom počte aspektov súkromného života dotknutých osôb vrátane citlivých informácií, akými sú sexuálna orientácia, politické názory, náboženské, filozofické, spoločenské alebo iné presvedčenie a zdravotný stav, pričom takýmto údajom je navyše poskytnutá osobitná ochrana v práve Únie. Zo všetkých týchto údajov možno vyvodiť veľmi presné závery o súkromnom živote osôb, ktorých údaje boli uchovávané, 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. Konkrétne takéto údaje poskytujú prostriedky na vytvorenie profilu dotknutých osôb, čo je s ohľadom na právo na rešpektovanie súkromného života rovnako citlivá informácia, ako samotný obsah komunikácií (rozsudok z 5. apríla 2022, Commissioner of An Garda Síochána a i., C-140/20, EU:C:2022:258, bod 45, ako aj citovaná judikatúra).
- 62 Preto na jednej strane uchovávanie údajov o prenose dát a polohe na policajné účely môže zasahovať do práva na rešpektovanie komunikácie zakotveného v článku 7 Charty a odrádzať užívateľov elektronických komunikačných prostriedkov od uplatňovania ich slobody prejavu zaručenej v článku 11 Charty, pričom tieto účinky sú ešte závažnejšie vzhľadom na veľké množstvo a rôznorodosť uchovávaných údajov. Na druhej strane vzhľadom na značné množstvo údajov o prenose dát a polohe, ktoré možno priebežne uchovávať na základe opatrenia o všeobecnom a nediferencovanom uchovávaní, a na citlivú povahu informácií, ktoré sa dajú z týchto údajov získať, už samotné uchovávanie uvedených údajov poskytovateľmi elektronických komunikačných služieb v sebe zahŕňa riziká zneužitia a neoprávneného prístupu (rozsudok z 5. apríla 2022, Commissioner of An Garda Síochána a i., C-140/20, EU:C:2022:258, bod 46, ako aj citovaná judikatúra).
- 63 Článok 15 ods. 1 smernice 2002/58 však tým, že umožňuje členským štátom obmedziť práva a povinnosti stanovené v bodoch 51 až 54 tohto rozsudku, odráža skutočnosť, že práva zakotvené v článkoch 7, 8 a 11 Charty nie sú absolútnymi výsadami, ale musia sa vnímať vo vzťahu k ich úlohe v spoločnosti. Charta, ako vyplýva z jej článku 52 ods. 1, totiž pripúšťa obmedzenia výkonu týchto práv, pokiaľ sú tieto obmedzenia stanovené zákonom, rešpektujú podstatu uvedených práv a za predpokladu dodržiavania zásady proporcionality sú nevyhnutné a skutočne zodpovedajú cieľom všeobecného záujmu, ktoré sú uznané Úniou, alebo potrebe chrániť práva a slobody iných. Na účely výkladu článku 15 ods. 1 smernice 2002/58 so zreteľom na Chartu je teda potrebné zohľadniť tiež význam práv zakotvených v článkoch 3, 4, 6 a 7 Charty a dôležitosť cieľov ochrany národnej bezpečnosti a boja proti závažnej trestnej činnosti, ktoré prispievajú k ochrane práv a slobôd iných (rozsudok z 5. apríla 2022, Commissioner of An Garda Síochána a i., C-140/20, EU:C:2022:258, bod 48, ako aj citovaná judikatúra).
- 64 Pokiaľ teda ide konkrétne o účinný boj proti trestným činom, ktorých obeťami sú najmä maloleté osoby a iné zraniteľné osoby, treba zohľadniť skutočnosť, že z článku 7 Charty môžu pre orgány verejnej moci vyplývať pozitívne povinnosti prijať právne opatrenia na ochranu súkromného a rodinného života. Takéto povinnosti môžu tiež vyplývať z uvedeného článku 7 v súvislosti s ochranou obydlia a komunikácie, ako aj z článku 3 v súvislosti s ochranou fyzickej a duševnej nedotknuteľnosti osôb a z článku 4 v súvislosti so zákazom mučenia a neľudského alebo ponižujúceho zaobchádzania (rozsudok z 5. apríla 2022, Commissioner of An Garda Síochána a i., C-140/20, EU:C:2022:258, bod 49, ako aj citovaná judikatúra).

- 65 Vzhľadom na tieto rôzne pozitívne povinnosti je teda potrebné pristúpiť k zosúladeniu rôznych legitímnych záujmov a dotknutých práv a vytvoriť právny rámec umožňujúci toto zosúladenie (pozri v tomto zmysle rozsudok z 5. apríla 2022, Commissioner of An Garda Síochána a i., C-140/20, EU:C:2022:258, bod 50, ako aj citovanú judikatúru).
- 66 V tomto rámci zo samotného znenia článku 15 ods. 1 prvej vety smernice 2002/58 vyplýva, že členské štáty môžu prijať opatrenie odchyľujúce sa od zásady dôvernosti uvedenej v bode 52 tohto rozsudku, ak je takéto opatrenie „nevyhnutné, vhodné a primerané v demokratickej spoločnosti“, pričom odôvodnenie 11 tejto smernice na tento účel uvádza, že opatrenie takejto povahy musí byť „prísne“ proporcionálne vo vzťahu k zamýšľanému účelu.
- 67 V tejto súvislosti treba pripomenúť, že ochrana základného práva na rešpektovanie súkromného života v súlade s ustálenou judikatúrou Súdneho dvora vyžaduje, aby výnimky a obmedzenia v súvislosti s ochranou osobných údajov nepôsobili nad rámec toho, čo je prísne nevyhnutné. Okrem toho nemožno sledovať cieľ všeobecného záujmu bez zohľadnenia skutočnosti, že musí byť zosúladený so základnými právami dotknutými daným opatrením, a to náležitým vyvážením cieľa všeobecného záujmu a dotknutých práv (rozsudok z 5. apríla 2022, Commissioner of An Garda Síochána a i., C-140/20, EU:C:2022:258, bod 52, ako aj citovaná judikatúra).
- 68 Z judikatúry Súdneho dvora konkrétne vyplýva, že možnosť členských štátov odôvodniť obmedzenie práv a povinností stanovených najmä v článkoch 5, 6 a 9 smernice 2002/58 treba posudzovať z hľadiska závažnosti zásahu, ktorý takéto obmedzenie spôsobuje, a musí sa overiť, či je dôležitosť cieľa všeobecného záujmu sledovaného týmto obmedzením priamo úmerná závažnosti zásahu (rozsudok z 5. apríla 2022, Commissioner of An Garda Síochána a i., C-140/20, EU:C:2022:258, bod 53, ako aj citovaná judikatúra).
- 69 Na účely splnenia požiadavky proporcionality musí vnútroštátna právna úprava stanoviť jasné a presné pravidlá, ktoré budú upravovať rozsah a uplatnenie predmetného opatrenia a ukladať minimálne požiadavky tak, aby osoby, ktorých osobné údaje sú dotknuté, mali dostatočné záruky umožňujúce účinne chrániť tieto údaje pred rizikami zneužitia. Táto právna úprava musí byť podľa vnútroštátneho práva právne záväzná a musí najmä vymedziť okolnosti a podmienky, za akých možno prijať opatrenie upravujúce spracúvanie takýchto údajov, čím zaručí, aby zásah nešiel nad rámec toho, čo je striktne nevyhnutné. Nevyhnutnosť disponovať takými zárukami je o to dôležitejšia v prípade, keď sú osobné údaje spracúvané automaticky, najmä ak existuje značné riziko neoprávneného prístupu k týmto údajom. Tieto úvahy platia najmä vtedy, keď ide o ochranu tejto osobitnej kategórie osobných údajov, ktorú tvoria citlivé údaje (rozsudok z 5. apríla 2022, Commissioner of An Garda Síochána a i., C-140/20, EU:C:2022:258, bod 54, ako aj citovaná judikatúra).
- 70 Vnútroštátna právna úprava stanovujúca uchovávanie osobných údajov tak musí vždy spĺňať objektívne kritériá, ktoré vymedzujú vzťah medzi údajmi, ktoré majú byť uchovávané, a sledovaným cieľom (rozsudok z 5. apríla 2022, Commissioner of An Garda Síochána a i., C-140/20, EU:C:2022:258, bod 55, ako aj citovaná judikatúra).
- 71 Pokiaľ ide o ciele všeobecného záujmu, ktoré môžu odôvodniť opatrenie prijaté na základe článku 15 ods. 1 smernice 2002/58, z judikatúry Súdneho dvora, najmä z rozsudku zo 6. októbra 2020, La Quadrature du Net a i. (C-511/18, C-512/18 a C-520/18, EU:C:2020:791), vyplýva, že v súlade so zásadou proporcionality existuje hierarchia medzi týmito cieľmi

v závislosti od ich dôležitosti a že dôležitosť cieľa sledovaného takýmto opatrením musí byť priamo úmerná závažnosti zásahu, ktorý z neho vyplýva (rozsudok z 5. apríla 2022, Commissioner of An Garda Síochána a i., C-140/20, EU:C:2022:258, bod 56).

- 72) Pokiaľ teda ide o ochranu národnej bezpečnosti, ktorej význam presahuje význam ostatných cieľov uvedených v článku 15 ods. 1 smernice 2002/58, Súdny dvor konštatoval, že toto ustanovenie v spojení s článkami 7, 8 a 11, ako aj s článkom 52 ods. 1 Charty nebráni legislatívnym opatreniam, ktoré na účely ochrany národnej bezpečnosti umožňujú prikázať poskytovateľom elektronických komunikačných služieb, aby vykonali všeobecné a nediferencované uchovávanie údajov o prenose dát a polohe v situáciách, keď dotknutý členský štát čelí vážnej hrozbe pre národnú bezpečnosť, ktorá sa javí ako skutočná a aktuálna alebo predvídateľná, pričom rozhodnutie o vydaní takéhoto príkazu môže byť účinne preskúmané zo strany súdu alebo nezávislého správneho orgánu, ktorého rozhodnutie má záväzný účinok, a cieľom tohto preskúmania bude overiť existenciu jednej z týchto situácií a dodržanie podmienok a záruk, ktoré musia byť stanovené, a uvedený príkaz možno vydať len na časovo obmedzené obdobie, ktoré je striktné nevyhnutné, s možnosťou jeho predĺženia, pokiaľ takáto hrozba pretrváva (rozsudok z 5. apríla 2022, Commissioner of An Garda Síochána a i., C-140/20, EU:C:2022:258, bod 58, ako aj citovaná judikatúra).
- 73) Pokiaľ ide o cieľ predchádzania, vyšetrovania, odhaľovania a stíhania trestných činov, Súdny dvor uviedol, že v súlade so zásadou proporcionality platí, že len boj proti závažnej trestnej činnosti a predchádzanie vážnym hrozbám pre verejnú bezpečnosť môže odôvodniť také závažné zásahy do základných práv zakotvených v článkoch 7 a 8 Charty, akými sú zásahy, ktoré zahŕňajú uchovávanie údajov o prenose dát a polohe. Preto iba zásahy do uvedených základných práv, ktoré nemajú závažnú povahu, môžu byť odôvodnené cieľom spočívajúcim v predchádzaní, vyšetrovaní, odhaľovaní a stíhaní trestných činov vo všeobecnosti (rozsudok z 5. apríla 2022, Commissioner of An Garda Síochána a i., C-140/20, EU:C:2022:258, bod 59, ako aj citovaná judikatúra).
- 74) Pokiaľ ide o cieľ boja proti závažnej trestnej činnosti, Súdny dvor rozhodol, že vnútroštátna právna úprava, ktorá na tento účel stanovuje všeobecné a nediferencované uchovávanie údajov o prenose dát a polohe, presahuje rámec toho, čo je striktné nevyhnutné, a nemožno ju v demokratickej spoločnosti považovať za odôvodnenú. Vzhľadom na citlivú povahu informácií, ktoré môžu poskytovať údaje o prenose dát a polohe, je totiž dôvernosc týchto údajov zásadná pre právo na rešpektovanie súkromného života. S prihliadnutím jednak na odrádzajúce účinky, ktoré môže mať uchovávanie týchto údajov na výkon základných práv zakotvených v článkoch 7 a 11 Charty a ktoré sú uvedené v bode 62 tohto rozsudku, a jednak na závažnosť zásahu, ktorý spôsobuje takéto uchovávanie, je teda v demokratickej spoločnosti potrebné, aby toto uchovávanie bolo, ako to stanovuje systém zavedený smernicou 2002/58, výnimkou a nie pravidlom, a aby tieto údaje nemohli byť uchovávané systematicky a priebežne. Tento záver platí, aj pokiaľ ide o ciele boja proti závažnej trestnej činnosti a predchádzania vážnym hrozbám pre verejnú bezpečnosť, ako aj dôležitosť, ktorú im treba priznať (rozsudok z 5. apríla 2022, Commissioner of An Garda Síochána a i., C-140/20, EU:C:2022:258, bod 65, ako aj citovaná judikatúra).
- 75) Súdny dvor naopak spresnil, že článok 15 ods. 1 smernice 2002/58 v spojení s článkami 7, 8 a 11, ako aj s článkom 52 ods. 1 Charty nebráni legislatívnym opatreniam, ktoré na účely boja proti závažnej trestnej činnosti a predchádzania vážnym hrozbám pre verejnú bezpečnosť stanovujú
- ciele uchovávanie údajov o prenose dát a polohe, ktoré je vymedzené na základe objektívnych a nediskriminačných faktorov, podľa kategórií dotknutých osôb alebo prostredníctvom

geografického kritéria, na časovo obmedzené obdobie, ktoré je striktne nevyhnutné, s možnosťou jeho predĺženia,

- všeobecné a nediferencované uchovávanie IP adries pridelených zdroju spojenia na časovo obmedzené obdobie, ktoré je striktne nevyhnutné,
- všeobecné a nediferencované uchovávanie údajov týkajúcich sa totožnosti užívateľov elektronických komunikačných prostriedkov a
- možnosť prikázať prostredníctvom rozhodnutia príslušného orgánu, ktoré podlieha účinnému súdnemu preskúmaniu, poskytovateľom elektronických komunikačných služieb, aby urýchlene uchovali (*quick freeze*) na potrebný čas údaje o prenose dát a polohe, ktoré majú k dispozícii,

pokiaľ tieto opatrenia prostredníctvom jasných a presných pravidiel zabezpečujú, že uchovávanie dotknutých údajov podlieha dodržiavaniu príslušných hmotnoprávných a procesných podmienok a že dotknuté osoby majú účinné záruky proti rizikám zneužitia (rozsudky zo 6. októbra 2020, *La Quadrature du Net a i.*, C-511/18, C-512/18 a C-520/18, EU:C:2020:791, bod 168, ako aj z 5. apríla 2022, *Commissioner of An Garda Síochána a i.*, C-140/20, EU:C:2022:258, bod 67).

O opatrení, ktoré stanovuje všeobecné a nediferencované uchovávanie väčšiny údajov o prenose dát a polohe po dobu niekoľkých týždňov

- 76 Práve s ohľadom na tieto zásadné úvahy treba preskúmať charakteristické znaky vnútroštátnej právnej úpravy dotknutej vo veci samej, na ktoré poukazuje vnútroštátny súd.
- 77 V prvom rade, pokiaľ ide o rozsah uchovávaných údajov, z návrhu na začatie prejudiciálneho konania vyplýva, že v rámci poskytovania telefónnych služieb sa povinnosť uchovávania stanovená touto právnou úpravou týka najmä údajov potrebných na identifikáciu zdroja spojenia a jeho určenia, dátumu a času začiatku a konca spojenia, alebo – v prípade komunikácie prostredníctvom krátkej textovej, multimediálnej alebo podobnej správy – okamihu odoslania a prijatia správy, ako aj v prípade mobilného spojenia, označenia buniek, ktoré sa v prípade volajúceho a volaného čísla použili na začiatku spojenia. V rámci poskytovania služieb prístupu k internetu sa povinnosť uchovávania vzťahuje okrem iného na IP adresu pridelenú účastníkovi, dátum a čas začiatku a konca používania internetu z pridelenej IP adresy a v prípade mobilného spojenia označenie buniek, ktoré sa použili na začiatku internetového spojenia. Uchovávajú sa tiež údaje, z ktorých vyplýva zemepisná poloha a maximálny dosah antén, ktoré využíva príslušná bunka.
- 78 Hoci vnútroštátna právna úprava dotknutá vo veci samej vylučuje z povinnosti uchovávania obsah komunikácie a údaje týkajúce sa navštívených internetových stránok a vyžaduje uchovávanie identifikátora bunky len na začiatku spojenia, treba poznamenať, že to isté v podstate platilo aj pre vnútroštátne právne predpisy preberajúce smernicu 2006/24, o ktoré išlo vo veciach, v ktorých bol vydaný rozsudok zo 6. októbra 2020, *La Quadrature du Net a i.* (C-511/18, C-512/18 a C-520/18, EU:C:2020:791). Napriek týmto obmedzeniam však Súdny dvor v tomto rozsudku rozhodol, že kategórie údajov uchovávaných na základe uvedenej smernice a týchto vnútroštátnych právnych predpisov môžu umožniť vyvodiť veľmi presné závery o súkromnom živote dotknutých osôb, ako sú 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, a najmä poskytnúť prostriedky na vytvorenie profilu týchto osôb.

- 79 Navyše treba konštatovať, že aj keď sa právna úprava dotknutá vo veci samej nevzťahuje na údaje týkajúce sa navštevovaných internetových stránok, stanovuje však uchovávanie IP adries. Keďže však IP adresy možno použiť na vystopovanie kompletného prechádzania stránok užívateľom internetu a následne jeho online aktivít, tieto údaje umožňujú vytvoriť podrobný profil tohto užívateľa. Uchovávanie a analýza uvedených IP adries, ktoré sú potrebné na takéto sledovanie, tak predstavujú závažné zásahy do základných práv užívateľa internetu zakotvených v článkoch 7 a 8 Charty (pozri v tomto zmysle rozsudok zo 6. októbra 2020, *La Quadrature du Net a i.*, C-511/18, C-512/18 a C-520/18, EU:C:2020:791, bod 153).
- 80 Okrem toho, ako uviedla SpaceNet vo svojich písomných pripomienkach, hoci sa na údaje týkajúce sa služieb elektronickej pošty nevzťahuje povinnosť uchovávanía stanovená právnou úpravou, o ktorú ide vo veci samej, predstavujú len nepatrnú časť predmetných údajov.
- 81 Ako v podstate uviedol generálny advokát v bode 60 svojich návrhov, povinnosť uchovávanía stanovená vnútroštátnou právnou úpravou, o ktorú ide vo veci samej, sa vzťahuje na veľmi široký súbor údajov o prenose dát a polohe, ktorý v podstate zodpovedá údajom, ktoré viedli k ustálenej judikatúre pripomenutej v bode 78 tohto rozsudku.
- 82 Navyše v odpovedi na otázku položenú na pojednávaní nemecká vláda spresnila, že len 1 300 subjektov je zaradených na zoznam osôb, orgánov alebo organizácií sociálnej alebo náboženskej povahy, ktorých údaje týkajúce sa elektronických komunikácií nie sú uchovávané podľa § 99 ods. 2 a § 113b ods. 6 TKG, čo zjavne predstavuje malú časť všetkých užívateľov telekomunikačných služieb v Nemecku, na ktorých údaje sa vzťahuje povinnosť uchovávanía stanovená vnútroštátnou právnou úpravou dotknutou vo veci samej. Uchovávajú sa tak aj údaje o užívateľoch, ktorí sú viazaní profesijným tajomstvom, ako sú advokáti, lekári a novinári.
- 83 Z rozhodnutia vnútroštátneho súdu teda vyplýva, že uchovávanie údajov o prenose dát a polohe stanovené touto vnútroštátnou právnou úpravou sa týka takmer všetkých osôb v populácii bez toho, aby sa tieto osoby, hoci aj nepriamo, nachádzali v situácii, ktorá by mohla viesť k trestnému stíhaniu. Rovnako tak stanovuje bezdôvodné, všeobecné a osobne, časovo a miestne nediferencované uchovávanie podstatnej časti údajov o prenose dát a polohe, ktorých rozsah v podstate zodpovedá rozsahu uchovávaných údajov vo veciach, v ktorých bola vydaná judikatúra uvedená v bode 78 tohto rozsudku.
- 84 Preto vzhľadom na judikatúru citovanú v bode 75 tohto rozsudku nemožno, na rozdiel od toho, čo tvrdí nemecká vláda, takúto povinnosť uchovávanía údajov, o akú ide vo veci samej, považovať za cielené uchovávanie údajov.
- 85 V druhom rade, pokiaľ ide o dobu uchovávanía údajov, z článku 15 ods. 1 druhej vety smernice 2002/58 vyplýva, že doba uchovávanía stanovená vnútroštátnym opatrením, ktoré ukladá všeobecnú a nediferencovanú povinnosť uchovávanía, je nepochybne jedným z relevantných faktorov na účely určenia, či právo Únie bráni takému opatreniu, pričom uvedená veta vyžaduje, aby táto doba bola „obmedzená“.
- 86 V prejednávanej veci je pritom pravda, že tieto doby, ktoré podľa § 113b ods. 1 TKG predstavujú štyri týždne v prípade údajov o polohe a desať týždňov v prípade iných údajov, sú citeľne kratšie ako tie, ktoré stanovujú vnútroštátne právne predpisy stanovujúce povinnosť všeobecného a nediferencovaného uchovávanía, ktoré Súdny dvor posudzoval v rozsudkoch

z 21. decembra 2016, Tele2 Sverige a Watson a i. (C-203/15 a C-698/15, EU:C:2016:970); zo 6. októbra 2020, La Quadrature du Net a i. (C-511/18, C-512/18 a C-520/18, EU:C:2020:791), ako aj z 5. apríla 2022, Commissioner of An Garda Síochána a i. (C-140/20, EU:C:2022:258).

- 87 Ako však vyplýva z judikatúry citovanej v bode 61 tohto rozsudku, závažnosť zásahu vyplýva z rizika, najmä vzhľadom na ich počet a rôznorodosť, že uchovávané údaje ako celok umožňujú vyvodiť veľmi presné závery o súkromnom živote osoby alebo osôb, ktorých údaje boli uchovávané, a najmä poskytujú prostriedky na vytvorenie profilu dotknutej osoby alebo osôb, ktorý je z hľadiska práva na rešpektovanie súkromného života rovnako citlivou informáciou ako samotný obsah komunikácií.
- 88 Uchovávanie údajov o prenose dát a polohe, ktoré môžu poskytnúť informácie o komunikácii uskutočnenej užívateľom prostriedku elektronickej komunikácie alebo o polohe koncových zariadení, ktoré používa, má teda v každom prípade závažnú povahu bez ohľadu na dĺžku obdobia uchovávaní, množstvo či povahu uchovávaných údajov, pokiaľ z uvedeného súboru údajov možno vyvodiť presné závery o súkromnom živote dotknutej osoby alebo dotknutých osôb [pokiaľ ide o prístup k takýmto údajom, pozri rozsudok z 2. marca 2021, Prokuratuur (Podmienky prístupu k údajom týkajúcim sa elektronických komunikácií), C-746/18, EU:C:2021:152, bod 39].
- 89 V tejto súvislosti treba uviesť, že aj na základe uchovávaní obmedzeného množstva údajov o prenose dát a polohe alebo uchovávaní týchto údajov počas krátkeho obdobia možno získať veľmi presné informácie o súkromnom živote užívateľa prostriedku elektronickej komunikácie. Okrem toho množstvo dostupných údajov a veľmi presné informácie o súkromnom živote dotknutej osoby, ktoré z nich vyplývajú, možno posúdiť až po nahliadnutí do uvedených údajov. K zásahu vyplývajúcu z uchovávaní uvedených údajov pritom nevyhnutne dochádza predtým, než je možné nahliadnúť do údajov a informácií, ktoré z nich vyplývajú. Posúdenie závažnosti zásahu, ktorý prístup predstavuje, sa tak nevyhnutne vykonáva v závislosti od všeobecného rizika vzťahujúceho sa na kategóriu uchovávaných údajov pre súkromný život dotknutých osôb bez toho, aby bolo okrem toho potrebné vedieť, či informácie týkajúce sa súkromného života, ktoré z neho vyplývajú, konkrétne majú alebo nemajú citlivú povahu [pozri v tomto zmysle rozsudok z 2. marca 2021, Prokuratuur (Podmienky prístupu k údajom týkajúcim sa elektronických komunikácií), C-746/18, EU:C:2021:152, bod 40].
- 90 V prejednávanej veci, ako vyplýva z bodu 77 tohto rozsudku a ako bolo potvrdené na pojednávaní, súbor údajov o prenose dát uchovávaných počas desiatich týždňov a údajov o polohe uchovávaných počas štyroch týždňov umožňuje vyvodiť veľmi presné závery o súkromnom živote osôb, ktorých údaje sa uchovávajú, ako sú 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, a najmä vytvoriť profil uvedených osôb.
- 91 V treťom rade, pokiaľ ide o záruky stanovené vnútroštátnou právnou úpravou, o ktorú ide vo veci samej, ktorej cieľom je chrániť uchovávané údaje pred rizikami zneužitia a pred akýmkoľvek neoprávneným prístupom, treba uviesť, že uchovávanie týchto údajov a prístup k nim predstavujú, ako vyplýva z judikatúry pripomenutej v bode 60 tohto rozsudku, samostatné zásahy do základných práv zaručených článkami 7 a 11 Charty, ktoré si vyžadujú samostatné odôvodnenie podľa článku 52 ods. 1 tejto Charty. Z toho vyplýva, že vnútroštátna právna úprava, ktorá zabezpečuje plné dodržiavanie podmienok vyplývajúcich z judikatúry, ktorou sa vykladá smernica 2002/58, pokiaľ ide o prístup k uchovávaným údajom, nemôže svojou povahou obmedziť alebo dokonca napraviť závažný zásah do práv zaručených v článkoch 5 a 6 tejto

smernice a základnými právami konkretizovanými týmito článkami, ktorý by vyplýval zo všeobecného uchovávanía týchto údajov stanoveného touto vnútroštátnou právnou úpravou (rozsudok z 5. apríla 2022, Commissioner of An Garda Síochána a i., C-140/20, EU:C:2022:258, bod 47).

- 92 Napokon v štvrtom rade, pokiaľ ide o tvrdenie Európskej komisie, že obzvlášť závažnú trestnú činnosť možno prirovnať k hrozbe pre národnú bezpečnosť, Súdny dvor už rozhodol, že cieľ spočívajúci v ochrane národnej bezpečnosti zodpovedá prvoradému záujmu chrániť základné funkcie štátu a základné záujmy spoločnosti predchádzaním a potláčaním činností, ktoré môžu vážne destabilizovať základné ústavné, politické, hospodárske alebo sociálne štruktúry krajiny, a najmä priamo ohroziť spoločnosť, obyvateľstvo alebo štát ako také, akými sú najmä teroristické aktivity (rozsudok z 5. apríla 2022, Commissioner of An Garda Síochána a i., C-140/20, EU:C:2022:258, bod 61, ako aj citovaná judikatúra).
- 93 Na rozdiel od trestnej činnosti, hoci aj obzvlášť závažnej, musí byť hrozba pre národnú bezpečnosť skutočná a aktuálna, alebo prinajmenšom predvídateľná, čo predpokladá existenciu dostatočne konkrétnych okolností, aby bolo možné odôvodniť opatrenie všeobecného a nediferencovaného uchovávanía údajov o prenose dát a polohe počas obmedzeného obdobia. Takáto hrozba sa teda svojou povahou, závažnosťou a osobitnou povahou okolností, ktoré ju tvoria, odlišuje od všeobecného a trvalého rizika, ktorým je riziko vzniku napätia alebo narušenia, a to aj závažného, v oblasti verejnej bezpečnosti, alebo riziko závažných trestných činov (rozsudok z 5. apríla 2022, Commissioner of An Garda Síochána a i., C-140/20, EU:C:2022:258, bod 62, ako aj citovaná judikatúra).
- 94 Trestnú činnosť, a to ani obzvlášť závažnú, teda nemožno prirovnať k hrozbe pre národnú bezpečnosť. Takéto prirovnanie by mohlo zaviesť kategóriu nachádzajúcu sa na rozhraní národnej bezpečnosti a verejnej bezpečnosti s cieľom uplatniť na verejnú bezpečnosť požiadavky, ktoré sú spojené s národnou bezpečnosťou (rozsudok z 5. apríla 2022, Commissioner of An Garda Síochána a i., C-140/20, EU:C:2022:258, bod 63).

O opatreniach, ktoré stanovujú ciele uchovávanie, urýchléné uchovávanie alebo uchovávanie IP adries

- 95 Viaceré vlády vrátane francúzskej vlády zdôrazňujú, že jedine všeobecné a nediferencované uchovávanie umožňuje účinné dosiahnutie cieľov sledovaných opatreniami stanovujúcimi uchovávanie, zatiaľ čo nemecká vláda v podstate spresňuje, že takýto záver nie je vyvrátený skutočnosťou, že členské štáty môžu použiť opatrenia stanovujúce ciele uchovávanie a urýchléné uchovávanie, ktoré sú uvedené v bode 75 tohto rozsudku.
- 96 V tejto súvislosti treba v prvom rade uviesť, že účinnosť trestného stíhania vo všeobecnosti nezávisí od jediného vyšetrovacieho nástroja, ale od všetkých vyšetrovacích nástrojov, ktorými na tento účel disponujú príslušné vnútroštátne orgány (rozsudok z 5. apríla 2022, Commissioner of An Garda Síochána a i., C-140/20, EU:C:2022:258, bod 69).
- 97 V druhom rade článok 15 ods. 1 smernice 2002/58 v spojení s článkami 7, 8 a 11, ako aj s článkom 52 ods. 1 Charty, ako bol vyložený judikatúrou pripomenutou v bode 75 tohto rozsudku, umožňuje členským štátom prijať na účely boja proti závažnej trestnej činnosti a predchádzania vážnym hrozbám pre verejnú bezpečnosť nielen opatrenia zavádzajúce ciele uchovávanie a urýchléné uchovávanie, ale aj opatrenia stanovujúce všeobecné a nediferencované

uchovávanie jednak údajov týkajúcich sa totožnosti užívateľov elektronických komunikačných prostriedkov a jednak IP adries pridelených zdroju spojenia (rozsudok z 5. apríla 2022, Commissioner of An Garda Síochána a i., C-140/20, EU:C:2022:258, bod 70).

- 98 V tejto súvislosti je nesporné, že uchovávanie údajov týkajúcich sa občianskej totožnosti užívateľov prostriedkov elektronickej komunikácie môže prispieť k boju proti závažnej trestnej činnosti, pokiaľ tieto údaje umožňujú identifikovať osoby, ktoré použili takéto prostriedky v súvislosti s prípravou alebo spáchaním činu spadajúceho pod závažnú trestnú činnosť (rozsudok z 5. apríla 2022, Commissioner of An Garda Síochána a i., C-140/20, EU:C:2022:258, bod 71).
- 99 Smernica 2002/58 však na účely boja proti trestnej činnosti vo všeobecnosti nebráni všeobecnému uchovávaniu údajov týkajúcich sa totožnosti. Za týchto podmienok treba spresniť, že ani táto smernica, ani nijaký iný akt práva Únie nebránia vnútroštátnej právnej úprave, ktorej predmetom je boj proti závažnej trestnej činnosti, podľa ktorej je získanie prostriedku elektronickej komunikácie, akým je predplatená SIM karta, podmienené overením úradných dokladov preukazujúcich totožnosť kupujúceho a zaznamenaním informácií, ktoré z toho vyplývajú, predávajúcim, pričom predávajúci má prípadne povinnosť sprístupniť tieto informácie príslušným vnútroštátnym orgánom (rozsudok z 5. apríla 2022, Commissioner of An Garda Síochána a i., C-140/20, EU:C:2022:258, bod 72).
- 100 Okrem toho treba pripomenúť, že všeobecné uchovávanie IP adries pridelených zdroju spojenia predstavuje závažný zásah do základných práv zakotvených v článkoch 7 a 8 Charty, keďže z týchto IP adries možno vyvodiť presné závery o súkromnom živote dotknutého užívateľa elektronického telekomunikačného prostriedku a môže mať odradzujúce účinky na výkon slobody prejavu zaručenej článkom 11 Charty. Pokiaľ však ide o takéto uchovávanie, Súdny dvor konštatoval, že na účely nevyhnutného zosúladenia predmetných práv a legitímnych záujmov vyžadovaných judikatúrou uvedenou v bodoch 65 až 68 tohto rozsudku je potrebné zohľadniť skutočnosť, že v prípade spáchania trestného činu online, a najmä v prípade nadobúdania, šírenia, ďalšieho postupovania alebo sprístupňovania detskej pornografie online v zmysle článku 2 písm. c) smernice Európskeho parlamentu a Rady 2011/93/EÚ z 13. decembra 2011 o boji proti sexuálnemu zneužívaniu a sexuálnemu vykorisťovaniu detí a proti detskej pornografii, ktorou sa nahrádza rámcové rozhodnutie Rady 2004/68/SVV (Ú. v. EÚ L 335, 2011, s. 1), môže IP adresa predstavovať jediný prostriedok vyšetrovania umožňujúci identifikáciu osoby, ktorej bola táto adresa pridelená v čase spáchania tohto trestného činu (rozsudok z 5. apríla 2022, Commissioner of An Garda Síochána a i., C-140/20, EU:C:2022:258, bod 73).
- 101 Hoci je za týchto podmienok pravda, že legislatívne opatrenie stanovujúce uchovávanie IP adries všetkých fyzických osôb, ktoré vlastnia koncové zariadenie umožňujúce prístup na internet, by sa týkalo osôb, ktoré na prvý pohľad nemajú žiadnu spojitosť so sledovanými cieľmi v zmysle judikatúry uvádzanej v bode 70 tohto rozsudku, a že užívatelia internetu majú v súlade s tým, čo bolo konštatované v bode 54 tohto rozsudku, právo očakávať na základe článkov 7 a 8 Charty, že ich totožnosť nebude v zásade odhalená, sa legislatívne opatrenie, ktoré stanovuje všeobecné a nediferencované uchovávanie výlučne IP adries pridelených zdroju spojenia, v zásade nejaví v rozpore s článkom 15 ods. 1 smernice 2002/58 v spojení s článkami 7, 8 a 11, ako aj s článkom 52 ods. 1 Charty, pokiaľ táto možnosť podlieha prísnemu dodržiavaniu hmotnoprávných a procesných podmienok, ktoré by mali upravovať použitie týchto údajov (rozsudok zo 6. októbra 2020, La Quadrature du Net a i., C-511/18, C-512/18 a C-520/18, EU:C:2020:791, bod 155).

- 102 Vzhľadom na závažnosť zásahu do základných práv zakotvených v článkoch 7 a 8 Charty, ktorý predstavuje toto uchovávanie údajov, môže len boj proti závažnej trestnej činnosti a predchádzanie vážnym hrozbám pre verejnú bezpečnosť odôvodňovať takýto zásah. Okrem toho doba uchovávania nemôže trvať dlhšie, než je striktné nevyhnutné vzhľadom na sledovaný cieľ. Napokon musí opatrenie tejto povahy stanoviť prísne podmienky a záruky týkajúce sa použitia týchto údajov, najmä prostredníctvom sledovania komunikácie a činností, ktoré dotknuté osoby vykonávajú online (rozsudok zo 6. októbra 2020, *La Quadrature du Net a i.* (C-511/18, C-512/18 a C-520/18, EU:C:2020:791, bod 156).
- 103 Na rozdiel od toho, na čo poukázal vnútroštátny súd, tak medzi bodmi 155 a 168 rozsudku zo 6. októbra 2020, *La Quadrature du Net a i.* (C-511/18, C-512/18 a C-520/18, EU:C:2020:791), neexistuje napätie. Ako totiž v podstate uviedol generálny advokát v bodoch 81 a 82 svojich návrhov, z bodu 155 v spojení s bodom 156 a bodom 168 tohto rozsudku jasne vyplýva, že len boj proti závažnej trestnej činnosti a predchádzanie vážnym hrozbám pre verejnú bezpečnosť môžu podobne ako ochrana národnej bezpečnosti odôvodniť všeobecné uchovávanie IP adries pridelených zdroju spojenia bez ohľadu na to, či dotknuté osoby môžu mať aspoň nepriamu súvislosť so sledovanými cieľmi.
- 104 V treťom rade, pokiaľ ide o legislatívne opatrenia stanovujúce cielené uchovávanie a urýchlené uchovávanie údajov o prenose dát a polohe, z niektorých námietok členských štátov proti takýmto opatreniam je zjavné užšie chápanie rozsahu týchto opatrení, než je to, ktoré je stanovené v judikatúre pripomenutej v bode 75 tohto rozsudku. Hoci totiž v súlade s tým, čo bolo pripomenuté v bode 57 tohto rozsudku, tieto opatrenia na uchovávanie údajov musia mať v systéme zavedenom smernicou 2002/58 povahu výnimky, táto smernica v spojení so základnými právami zakotvenými v článkoch 7, 8 a 11, ako aj v článku 52 ods. 1 Charty nepodmieňuje možnosť vydať súdny príkaz ukladajúci cielené uchovávanie predchádzajúcou znalosťou miest, kde by mohlo dôjsť k závažnej trestnej činnosti, alebo osôb podozrivých z účasti na takejto trestnej činnosti. Uvedená smernica rovnako nevyžaduje, aby bol súdny príkaz požadujúci urýchlené uchovávanie obmedzený na podozrivé osoby identifikované pred vydaním takéhoto príkazu (rozsudok z 5. apríla 2022, *Commissioner of An Garda Síochána a i.*, C-140/20, EU:C:2022:258, bod 75).
- 105 Pokiaľ ide po prvé o cielené uchovávanie, Súdny dvor rozhodol, že článok 15 ods. 1 smernice 2002/58 nebráni vnútroštátnej právnej úprave založenej na objektívnych skutočnostiach, ktorá umožňuje zamerať sa na jednej strane na osoby, ktorých údaje o prenose dát a polohe môžu aspoň nepriamo súvisieť so závažnou trestnou činnosťou, prispieť k boju proti závažnej trestnej činnosti alebo predchádzať vážnemu nebezpečenstvu pre verejnú bezpečnosť či dokonca nebezpečenstvu pre národnú bezpečnosť (rozsudok z 5. apríla 2022, *Commissioner of An Garda Síochána a i.*, C-140/20, EU:C:2022:258, bod 76, ako aj citovaná judikatúra).
- 106 Súdny dvor v tejto súvislosti spresnil, že hoci sa tieto objektívne skutočnosti môžu líšiť v závislosti od opatrení prijatých na účely predchádzania, vyšetrovania, odhaľovania a stíhania závažnej trestnej činnosti, takto vymedzenými osobami môžu byť najmä osoby, ktoré boli v rámci uplatniteľných vnútroštátnych postupov a na základe objektívnych a nediskriminačných faktorov vopred identifikované ako osoby, ktoré predstavujú hrozbu pre verejnú bezpečnosť alebo národnú bezpečnosť dotknutého členského štátu (rozsudok z 5. apríla 2022, *Commissioner of An Garda Síochána a i.*, C-140/20, EU:C:2022:258, bod 77).

- 107 Členské štáty tak majú okrem iného možnosť prijať opatrenia na uchovávanie údajov týkajúcich sa osôb, ktoré sú na základe takejto identifikácie predmetom vyšetrovania, alebo iných súčasných opatrení dohľadu alebo zápisu do vnútroštátneho registra trestov, v ktorých je uvedené predchádzajúce odsúdenie za závažnú trestnú činnosť, ktorá môže predstavovať vysoké riziko opakovania trestnej činnosti. Ak je však takáto identifikácia založená na objektívnych a nediskriminačných faktoroch definovaných vnútroštátnym právom, cielené uchovávanie údajov zamerané na takto identifikované osoby je odôvodnené (rozsudok z 5. apríla 2022, Commissioner of An Garda Síochána a i., C-140/20, EU:C:2022:258, bod 78).
- 108 Na druhej strane opatrenie na cielené uchovávanie údajov o prenose dát a polohe môže byť podľa voľby vnútroštátneho zákonodarcu a pri prísnom dodržaní zásady proporcionality založené aj na geografickom kritériu, ak sa príslušné vnútroštátne orgány na základe objektívnych a nediskriminačných faktorov domnievajú, že v jednej alebo vo viacerých zemepisných oblastiach existuje zvýšené riziko prípravy alebo páchania závažných trestných činov. Medzi tieto oblasti môžu patriť najmä miesta s vysokým výskytom závažných trestných činov, miesta, ktoré sú v osobitnej miere vystavené páchaniu závažnej trestnej činnosti, akými sú miesta alebo infraštruktúry pravidelne navštevované veľkým počtom osôb, alebo tiež strategické miesta, akými sú letiská, stanice, námorné prístavy alebo oblasti platenia mýta (rozsudok z 5. apríla 2022, Commissioner of An Garda Síochána a i., C-140/20, EU:C:2022:258, bod 79, ako aj citovaná judikatúra).
- 109 Treba zdôrazniť, že podľa tejto judikatúry môžu príslušné vnútroštátne orgány prijať pre oblasti uvedené v predchádzajúcom bode opatrenie na cielené uchovávanie údajov založené na geografickom kritériu, akým je najmä priemerná miera trestnej činnosti v zemepisnej oblasti, bez toho, aby nevyhnutne disponovali konkrétnymi ukazovateľmi týkajúcimi sa prípravy alebo páchania závažnej trestnej činnosti v dotknutých oblastiach. Keďže cielené uchovávanie údajov založené na takomto kritériu sa môže v závislosti od uvedených závažných trestných činov a situácie jednotlivých členských štátov dotýkať tak miest s vysokým výskytom závažných trestných činov, ako aj oblastí osobitne vystavených páchaniu takýchto činov, v zásade nemôže viesť ani k diskriminácii, keďže kritérium založené na priemernej miere závažnej trestnej činnosti samo osebe nijako nesúvisí s potenciálne diskriminačnými prvkami (rozsudok z 5. apríla 2022, Commissioner of An Garda Síochána a i., C-140/20, EU:C:2022:258, bod 80).
- 110 Okrem toho a predovšetkým opatrenie na cielené uchovávanie zamerané na miesta alebo infraštruktúry pravidelne navštevované veľkým počtom osôb, alebo tiež na strategické miesta, akými sú letiská, stanice, námorné prístavy alebo oblasti platenia mýta, umožňuje príslušným orgánom zhromažďovať údaje o prenose dát, a najmä údaje o polohe všetkých osôb, ktoré v danom čase používajú prostriedok elektronickej komunikácie na jednom z týchto miest. Takéto opatrenie na cielené uchovávanie tak môže uvedeným orgánom umožniť získať prostredníctvom prístupu k takto uchovávaným údajom informácie o prítomnosti týchto osôb na miestach alebo v zemepisných oblastiach, na ktoré sa toto opatrenie vzťahuje, ako aj o ich premiestňovaní medzi nimi alebo v rámci nich a na účely boja proti závažnej trestnej činnosti z toho vyvodiť závery o ich prítomnosti a činnosti na týchto miestach alebo v týchto zemepisných oblastiach v danom čase počas obdobia uchovávania (rozsudok z 5. apríla 2022, Commissioner of An Garda Síochána a i., C-140/20, EU:C:2022:258, bod 81).
- 111 Treba ešte uviesť, že zemepisné oblasti, na ktoré sa vzťahuje takéto cielené uchovávanie, môžu a prípadne musia byť zmenené v závislosti od vývoja podmienok, ktoré odôvodnili ich výber, čo umožní najmä reagovať na vývoj boja proti závažnej trestnej činnosti. Súdny dvor už rozhodol, že trvanie opatrení na cielené uchovávanie údajov, opísaných v bodoch 105 až 110 tohto rozsudku,

- nemôže prekročiť dobu, ktorá je striktné nevyhnutná vzhľadom na sledovaný cieľ, ako aj okolnosti, ktoré odôvodňujú tieto opatrenia, pričom tým nie je dotknutá možnosť ich obnovenia z dôvodu pretrvávajúcej potreby takéhoto uchovávanía (rozsudky zo 6. októbra 2020, *La Quadrature du Net a i.*, C-511/18, C-512/18 a C-520/18, EU:C:2020:791, bod 151, ako aj z 5. apríla 2022, *Commissioner of An Garda Síochána a i.*, C-140/20, EU:C:2022:258, bod 82).
- 112 Pokiaľ ide o možnosť stanoviť iné rozlišovacie kritériá, než je osobné alebo geografické kritérium, na účely cieleného uchovávanía údajov o prenose dát a polohe, nemožno vylúčiť, že sa môžu zohľadniť iné – objektívne a nediskriminačné – kritériá na zabezpečenie toho, aby sa rozsah cieleného uchovávanía obmedzil na to, čo je striktné nevyhnutné, a na to, aby sa aspoň nepriamo preukázala súvislosť medzi závažnou trestnou činnosťou a osobami, ktorých údaje sa uchovávajú. Vzhľadom na to, že článok 15 ods. 1 smernice 2002/58 sa týka právnych opatrení členských štátov, určenie takýchto kritérií prináleží členským štátom, a nie Súdnemu dvoru, pričom týmto spôsobom nemožno znovu zaviesť všeobecné a nediferencované uchovávanie údajov o prenose dát a polohe (rozsudok z 5. apríla 2022, *Commissioner of An Garda Síochána a i.*, C-140/20, EU:C:2022:258, bod 83).
- 113 V každom prípade, ako uviedol generálny advokát v bode 50 svojich návrhov, prípadná existencia ťažkostí pri presnej definícii prípadov a podmienok, za ktorých možno vykonávať cielené uchovávanie, nemôže odôvodniť to, aby členské štáty urobili z výnimky pravidlo a stanovili všeobecné a nediferencované uchovávanie údajov o prenose dát a polohe (rozsudok z 5. apríla 2022, *Commissioner of An Garda Síochána a i.*, C-140/20, EU:C:2022:258, bod 84).
- 114 Pokiaľ ide po druhé o urýchlené uchovávanie údajov o prenose dát a polohe spracúvaných a uložených poskytovateľmi elektronických komunikačných služieb na základe článkov 5, 6 a 9 smernice 2002/58 alebo na základe legislatívnych opatrení prijatých na základe článku 15 ods. 1 tejto smernice, treba pripomenúť, že takéto údaje sa v zásade musia podľa okolností vymazať alebo anonymizovať po uplynutí zákonných lehôt, v rámci ktorých sa má v súlade s vnútroštátnymi ustanoveniami, ktorými sa uvedená smernica preberá, uskutočniť ich spracovanie a uchovávanie. Súdny dvor rozhodol, že počas tohto spracúvanía a uchovávanía však môžu nastať situácie, keď je potrebné uchovať uvedené údaje aj po uplynutí týchto lehôt na účely objasnenía závažných trestných činov alebo narušení v oblasti národnej bezpečnosti, a to tak v situácii, keď už mohli byť tieto trestné činy alebo narušenia zistené, ako aj vtedy, keď po objektívnom preskúmaní všetkých relevantných okolností existuje o nich dôvodné podozrenie (rozsudok z 5. apríla 2022, *Commissioner of An Garda Síochána a i.*, C-140/20, EU:C:2022:258, bod 85).
- 115 V takejto situácii je vzhľadom na nevyhnutné zosúladenie dotknutých práv a záujmov uvedené v bodoch 65 až 68 tohto rozsudku prípustné, aby členské štáty stanovili v právnej úprave prijatej na základe článku 15 ods. 1 smernice 2002/58 možnosť nariadiť prostredníctvom rozhodnutia príslušného orgánu, ktoré podlieha účinnému súdnemu preskúmaniu, poskytovateľom elektronických komunikačných služieb, aby urýchlene uchovali na potrebný čas údaje o prenose dát a polohe, ktoré majú k dispozícii (rozsudky zo 6. októbra 2020, *La Quadrature du Net a i.*, C-511/18, C-512/18 a C-520/18, EU:C:2020:791, bod 163, ako aj z 5. apríla 2022, *Commissioner of An Garda Síochána a i.*, C-140/20, EU:C:2022:258, bod 86).
- 116 Keďže účel takéhoto urýchléného uchovávanía už nezodpovedá účelu, na ktorý sa údaje pôvodne zhromaždili a uchovávali, a keďže každé spracovanie údajov musí podľa článku 8 ods. 2 Charty zodpovedať konkrétnym cieľom, členské štáty musia vo svojich právnych predpisoch spresniť, na aké účely môže dôjsť k urýchlénému uchovávaniu údajov. Vzhľadom na závažnosť zásahu do

základných práv zakotvených v článkoch 7 a 8 Charty, ktorý môže predstavovať takéto uchovávanie, iba boj proti závažnej trestnej činnosti a *a fortiori* ochrana národnej bezpečnosti môžu odôvodniť tento zásah pod podmienkou, že toto opatrenie, ako aj prístup k takto uchovávaným údajom neprekračujú rámec toho, čo je striktne nevyhnutné, ako je uvedené v bodoch 164 až 167 rozsudku zo 6. októbra 2020, La Quadrature du Net a i. (C-511/18, C-512/18 a C-520/18, EU:C:2020:791) (rozsudok z 5. apríla 2022, Commissioner of An Garda Síochána a i., C-140/20, EU:C:2022:258, bod 87).

- 117 Súdny dvor spresnil, že opatrenie na uchovávanie údajov tejto povahy sa nesmie obmedzovať na údaje osôb, ktoré boli vopred identifikované ako osoby, ktoré predstavujú hrozbu pre verejnú bezpečnosť alebo národnú bezpečnosť dotknutého členského štátu, alebo osôb konkrétne podozrivých zo spáchania závažného trestného činu alebo ohrozenia národnej bezpečnosti. Podľa Súdneho dvora sa totiž v súlade s rámcom stanoveným v článku 15 ods. 1 smernice 2002/58 v spojení s článkami 7, 8 a 11, ako aj s článkom 52 ods. 1 Charty a vzhľadom na úvahy uvedené v bode 70 tohto rozsudku takéto opatrenie môže v závislosti od voľby vnútroštátneho zákonodarcu a pri dodržaní toho, čo je striktne nevyhnutné, rozšíriť na údaje o prenose dát a polohe týkajúce sa iných osôb, než sú osoby podozrivé z plánovania alebo spáchania závažného trestného činu alebo narušenia v oblasti národnej bezpečnosti, pokiaľ tieto údaje môžu na základe objektívnych a nediskriminačných faktorov prispieť k objasneniu takéhoto trestného činu alebo narušenia v oblasti národnej bezpečnosti, ako sú napríklad údaje týkajúce sa obete tohto činu, ako aj osôb z jej spoločenského alebo profesijného okolia (rozsudky zo 6. októbra 2020, La Quadrature du Net a i., C-511/18, C-512/18 a C-520/18, EU:C:2020:791, bod 165, ako aj z 5. apríla 2022, Commissioner of An Garda Síochána a i., C-140/20, EU:C:2022:258, bod 88).
- 118 Legislatívne opatrenie tak môže umožniť, aby sa poskytovateľom elektronických komunikačných služieb prikázalo urýchlené uchovávanie údajov o prenose dát a polohe, najmä osôb, s ktorými bola obeť predtým, ako došlo k vážnej hrozbe pre verejnú bezpečnosť alebo k spáchaniu závažného trestného činu, v kontakte prostredníctvom svojich prostriedkov elektronickej komunikácie (rozsudok z 5. apríla 2022, Commissioner of An Garda Síochána a i., C-140/20, EU:C:2022:258, bod 89).
- 119 Takéto urýchlené uchovávanie možno podľa judikatúry Súdneho dvora pripomenutej v bode 117 tohto rozsudku a za rovnakých podmienok, aké sú uvedené v tomto bode, rozšíriť aj na konkrétne zemepisné oblasti, akými sú miesta spáchania a prípravy trestného činu alebo narušenia v oblasti príslušnej národnej bezpečnosti. Treba spresniť, že takéto opatrenie sa môže vzťahovať aj na údaje o prenose dát a polohe týkajúce sa miesta, kde osoba, ktorá je potenciálnou obeťou závažného trestného činu, zmizla, a to za predpokladu, že toto opatrenie, ako aj prístup k takto uchovávaným údajom, neprekračujú rámec toho, čo je striktne nevyhnutné na účely boja proti závažnej trestnej činnosti alebo ochrany národnej bezpečnosti, ako je uvedené v bodoch 164 až 167 rozsudku zo 6. októbra 2020, La Quadrature du Net a i. (C-511/18, C-512/18 a C-520/18, EU:C:2020:791) (rozsudok z 5. apríla 2022, Commissioner of An Garda Síochána a i., C-140/20, EU:C:2022:258, bod 90).
- 120 Okrem toho treba spresniť, že článok 15 ods. 1 smernice 2002/58 nebráni tomu, aby príslušné vnútroštátne orgány nariadili opatrenie na rýchle uchovávanie už v prvom štádiu vyšetrovania týkajúceho sa vážnej hrozby pre verejnú bezpečnosť alebo možného závažného trestného činu, teda od okamihu, keď tieto orgány môžu podľa príslušných ustanovení vnútroštátneho práva začať takéto vyšetrovanie (rozsudok z 5. apríla 2022, Commissioner of An Garda Síochána a i., C-140/20, EU:C:2022:258, bod 91).

- 121 Pokiaľ ide ešte o rôznorodosť opatrení na uchovávanie údajov o prenose dát a polohe uvedených v bode 75 tohto rozsudku, treba spresniť, že tieto rôzne opatrenia sa môžu podľa voľby vnútroštátneho zákonodarcu a pri dodržaní toho, čo je striktné nevyhnutné, uplatniť spoločne. Za týchto podmienok článok 15 ods. 1 smernice 2002/58 v spojení s článkami 7, 8 a 11, ako aj s článkom 52 ods. 1 Charty, ako ho vykladá judikatúra vychádzajúca z rozsudku zo 6. októbra 2020, *La Quadrature du Net a i.* (C-511/18, C-512/18 a C-520/18, EU:C:2020:791), nebráni kombinácii týchto opatrení (rozsudok z 5. apríla 2022, *Commissioner of An Garda Síochána a i.*, C-140/20, EU:C:2022:258, bod 92).
- 122 Napokon po štvrté je dôležité zdôrazniť, že primeranosť opatrení prijatých podľa článku 15 ods. 1 smernice 2002/58 vyžaduje podľa ustálenej judikatúry Súdneho dvora, ako je zhrnutá v rozsudku zo 6. októbra 2020, *La Quadrature du Net a i.* (C-511/18, C-512/18 a C-520/18, EU:C:2020:791), dodržiavanie nielen požiadaviek spôsobilosti a nevyhnutnosti, ale aj požiadaviek, ktoré sa týkajú primeranosti týchto opatrení vo vzťahu k sledovanému cieľu (rozsudok z 5. apríla 2022, *Commissioner of An Garda Síochána a i.*, C-140/20, EU:C:2022:258, bod 93).
- 123 V tejto súvislosti treba pripomenúť, že Súdny dvor v bode 51 rozsudku z 8. apríla 2014, *Digital Rights Ireland a i.* (C-293/12 a C-594/12, EU:C:2014:238), rozhodol, že hoci má boj proti závažnej trestnej činnosti prvoradý význam na zabezpečenie verejnej bezpečnosti a jeho účinnosť môže vo veľkej miere závisieť od použitia moderných vyšetrovacích metód, takýto cieľ všeobecného záujmu, nech je akokoľvek zásadný, nemôže sám osebe odôvodniť to, aby sa opatrenie na všeobecné a nediferencované uchovávanie údajov o prenose dát a polohe, akým je opatrenie zavedené smernicou 2006/24, považovalo za nevyhnutné (rozsudok z 5. apríla 2022, *Commissioner of An Garda Síochána a i.*, C-140/20, EU:C:2022:258, bod 94).
- 124 V rovnakom zmysle Súdny dvor v bode 145 rozsudku zo 6. októbra 2020, *La Quadrature du Net a i.* (C-511/18, C-512/18 a C-520/18, EU:C:2020:791), spresnil, že dokonca ani pozitívne povinnosti členských štátov, ktoré môžu v závislosti od konkrétneho prípadu vyplývať z článkov 3, 4 a 7 Charty a ktoré sa týkajú, ako bolo uvedené v bode 64 tohto rozsudku, zavedenia pravidiel umožňujúcich účinný boj proti trestným činom, nemôžu viesť k odôvodneniu tak závažných zásahov, ako sú tie, ktoré spôsobuje vnútroštátna právna úprava stanovujúca uchovávanie údajov o prenose dát a polohe, do základných práv takmer celého obyvateľstva zakotvených v článkoch 7 a 8 Charty bez toho, aby existovala aspoň nepriama súvislosť medzi údajmi o dotknutých osobách a sledovaným cieľom (rozsudok z 5. apríla 2022, *Commissioner of An Garda Síochána a i.*, C-140/20, EU:C:2022:258, bod 95).
- 125 Okrem toho rozsudky ESLP z 25. mája 2021, *Big Brother Watch a i. v. Spojené kráľovstvo* (CE:ECHR:2021:0525JUD 005817013) a z 25. mája 2021 *Centrum för Rättvisa v. Švédsko* (CE:ECHR:2021:0525JUD 003525208), na ktoré sa odvolávali niektoré vlády na pojednávaní na účely tvrdenia, že EDLP nebráni vnútroštátnym právnym úpravám, ktoré v podstate stanovujú všeobecné a nediferencované uchovávanie údajov o prenose dát a polohe, nemôžu spochybniť výklad článku 15 ods. 1 smernice 2002/58 vyplývajúci z vyššie uvedených úvah. V týchto rozsudkoch totiž išlo o hromadné zachytávanie údajov súvisiacich s medzinárodnou komunikáciou. Ako teda uviedla Komisia na pojednávaní, Európsky súd pre ľudské práva sa v uvedených rozsudkoch nevyjadril k súladu všeobecného a nediferencovaného uchovávanie údajov o prenose dát a polohe na vnútroštátnom území, ani rozsiahleho zachycovania týchto údajov na účely predchádzania, odhaľovania a vyšetrovania závažných trestných činov, s EDLP. V každom prípade treba pripomenúť, že cieľom článku 52 ods. 3 Charty je zabezpečiť potrebnú súdržnosť medzi právami obsiahnutými v Charte a zodpovedajúcimi právami zaručenými EDLP bez toho, aby bola narušená autonómia práva Únie a Súdneho dvora Európskej únie, takže na

účely výkladu Charty treba zohľadniť zodpovedajúce práva vyplývajúce z EDLP iba ako minimálny stupeň ochrany (rozsudok zo 17. decembra 2020, Centraal Israëlitisch Consistorie van België a i., C-336/19, EU:C:2020:1031, bod 56).

O prístupe k údajom, ktoré boli uchovávané všeobecným a nediferencovaným spôsobom

- 126 Dánska vláda na pojednávaní tvrdila, že na účely boja proti závažnej trestnej činnosti by príslušné vnútroštátne orgány mali mať možnosť získať prístup k údajom o prenose dát a polohe, ktoré boli uchovávané všeobecným a nediferencovaným spôsobom v súlade s judikatúrou vyplývajúcou z rozsudku zo 6. októbra 2020, La Quadrature du Net a i. (C-511/18, C-512/18 a C-520/18, EU:C:2020:791, body 135 až 139), aby tak mohli čeliť vážnej hrozbe pre národnú bezpečnosť, ktorá sa javí ako skutočná a aktuálna alebo predvídateľná.
- 127 Na úvod treba uviesť, že ak by sa na účely boja proti závažnej trestnej činnosti umožnil prístup k údajom o prenose dát a polohe, ktoré boli uchovávané všeobecným a nediferencovaným spôsobom, viedlo by to k tomu, že tento prístup by závisel od okolností, ktoré nesúvisia s týmto cieľom, v závislosti od toho, či v dotknutom členskom štáte existuje alebo neexistuje vážna hrozba pre národnú bezpečnosť, ako je uvedené v predchádzajúcom bode, pričom vzhľadom na jediný cieľ boja proti závažnej trestnej činnosti, ktorý má odôvodňovať uchovávanie týchto údajov a prístup k nim, by nebolo odôvodnené rozdielne zaobchádzanie, najmä medzi členskými štátmi (rozsudok z 5. apríla 2022, Commissioner of An Garda Síochána a i., C-140/20, EU:C:2022:258, bod 97).
- 128 Ako už Súdny dvor rozhodol, prístup k údajom o prenose dát a polohe uchovávaným poskytovateľmi elektronických komunikačných služieb na základe opatrenia prijatého podľa článku 15 ods. 1 smernice 2002/58, ktorý sa musí uskutočniť pri úplnom rešpektovaní podmienok vyplývajúcich z judikatúry, ktorá vykladala túto smernicu, možno v zásade odôvodniť len cieľom všeobecného záujmu, pre ktorý bolo toto uchovávanie týmto poskytovateľom uložené. Inak je to len vtedy, ak význam cieľa sledovaného prístupom prekračuje význam cieľa, ktorý odôvodňuje uchovávanie (rozsudok z 5. apríla 2022, Commissioner of An Garda Síochána a i., C-140/20, EU:C:2022:258, bod 98).
- 129 Argumentácia dánskej vlády sa pritom týka situácie, v ktorej má cieľ zamýšľanej žiadosti o prístup, konkrétne boj proti závažnej trestnej činnosti, menší význam v hierarchii cieľov všeobecného záujmu než cieľ, ktorý odôvodňoval uchovávanie, konkrétne ochrana národnej bezpečnosti. Povoliť v takejto situácii prístup k uchovávaným údajom by bolo v rozpore s touto hierarchiou cieľov všeobecného záujmu, ktorá je pripomenutá v predchádzajúcom bode, ako aj v bodoch 68, 71, 72 a 73 tohto rozsudku (rozsudok z 5. apríla 2022, Commissioner of An Garda Síochána a i., C-140/20, EU:C:2022:258, bod 99).
- 130 Okrem toho a predovšetkým v súlade s judikatúrou pripomenutou v bode 74 tohto rozsudku údaje o prenose dát a polohe nemôžu byť predmetom všeobecného a nediferencovaného uchovávania na účely boja proti závažnej trestnej činnosti, a teda prístup k týmto údajom nemôže byť na takéto účely odôvodnený. Ak však boli tieto údaje výnimočne uchovávané všeobecným a nediferencovaným spôsobom na účely ochrany národnej bezpečnosti pred hrozbou, ktorá sa javí ako skutočná a aktuálna alebo predvídateľná za podmienok uvedených v bode 71 tohto rozsudku, príslušné vnútroštátne orgány v oblasti vyšetrovania trestných činov nemôžu mať prístup k uvedeným údajom v rámci trestného stíhania, lebo inak by bol zákaz vykonať takéto

uchovávanie na účely boja proti závažnej trestnej činnosti, ktorý je pripomenutý v uvedenom bode 74, zbavený akéhokoľvek potrebného účinku (rozsudok z 5. apríla 2022, Commissioner of An Garda Síochána a i., C-140/20, EU:C:2022:258, bod 100).

131 Vzhľadom na všetky predchádzajúce úvahy treba na prejudiciálnu otázku odpovedať tak, že článok 15 ods. 1 smernice 2002/58 v spojení s článkami 7, 8 a 11, ako aj s článkom 52 ods. 1 Charty sa má vykladať v tom zmysle, že bráni vnútroštátnym legislatívnym opatreniam, ktoré na účely boja proti závažnej trestnej činnosti a predchádzania vážnym hrozbám pre verejnú bezpečnosť preventívne stanovujú všeobecné a nediferencované uchovávanie údajov o prenose dát a polohe. Naopak, uvedený článok 15 ods. 1 v spojení s článkami 7, 8 a 11, ako aj s článkom 52 ods. 1 Charty sa má vykladať v tom zmysle, že nebráni vnútroštátnym legislatívnym opatreniam, ktoré:

- na účely ochrany národnej bezpečnosti umožňujú prikázať poskytovateľom elektronických komunikačných služieb, aby vykonali všeobecné a nediferencované uchovávanie údajov o prenose dát a polohe v situáciách, keď dotknutý členský štát čelí vážnej hrozbe pre národnú bezpečnosť, ktorá sa javí ako skutočná a aktuálna alebo predvídateľná, pričom rozhodnutie o vydaní takéhoto príkazu môže byť účinne preskúmané zo strany súdu alebo nezávislého správneho orgánu, ktorého rozhodnutie má záväzný účinok, a cieľom tohto preskúmania bude overiť existenciu jednej z týchto situácií a dodržanie podmienok a záruk, ktoré musia byť stanovené, a uvedený príkaz možno vydať len na časovo obmedzené obdobie, ktoré je striktne nevyhnutné, s možnosťou jeho predĺženia, pokiaľ takáto hrozba pretrváva,
- na účely ochrany národnej bezpečnosti, boja proti závažnej trestnej činnosti a predchádzania vážnym hrozbám pre verejnú bezpečnosť stanovujú ciele uchovávanie údajov o prenose dát a polohe, ktoré je vymedzené na základe objektívnych a nediskriminačných faktorov, podľa kategórií dotknutých osôb alebo prostredníctvom geografického kritéria, na časovo obmedzené obdobie, ktoré je striktne nevyhnutné, s možnosťou jeho predĺženia,
- na účely ochrany národnej bezpečnosti, boja proti závažnej trestnej činnosti a predchádzania vážnym hrozbám pre verejnú bezpečnosť stanovujú všeobecné a nediferencované uchovávanie IP adries pridelených zdroju spojenia na časovo obmedzené obdobie, ktoré je striktne nevyhnutné,
- na účely ochrany národnej bezpečnosti, boja proti trestnej činnosti a ochrany verejnej bezpečnosti stanovujú všeobecné a nediferencované uchovávanie údajov týkajúcich sa totožnosti užívateľov prostriedkov elektronickej komunikácie a
- na účely boja proti závažnej trestnej činnosti a *a fortiori* ochrany národnej bezpečnosti umožňujú prostredníctvom rozhodnutia príslušného orgánu, ktoré podlieha účinnému súdному preskúmaniu, prikázať poskytovateľom elektronických komunikačných služieb, aby urýchlene uchovali na potrebný čas údaje o prenose dát a polohe, ktoré majú k dispozícii,

pokiaľ tieto opatrenia prostredníctvom jasných a presných pravidiel zabezpečujú, že uchovávanie dotknutých údajov podlieha dodržiavaniu príslušných hmotnoprávných a procesných podmienok a že dotknuté osoby majú účinné záruky proti rizikám zneužitia.

O trovách

- 132 Vzhľadom na to, že konanie pred Súdny dvorom má vo vzťahu k účastníkom konania vo veci samej incidenčný charakter a bolo začaté v súvislosti s prekážkou postupu v konaní pred vnútroštátnym súdom, o trovách konania rozhodne tento vnútroštátny súd. Iné trovy konania, ktoré vznikli v súvislosti s predložením pripomienok Súdnemu dvoru a nie sú trovami uvedených účastníkov konania, nemôžu byť nahradené.

Z týchto dôvodov Súdny dvor (veľká komora) rozhodol 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 a 11, ako aj s článkom 52 ods. 1 Charty základných práv Európskej únie

sa má vykladať v tom zmysle, že:

bráni vnútroštátnym legislatívnym opatreniam, ktoré na účely boja proti závažnej trestnej činnosti a predchádzania vážnym hrozbám pre verejnú bezpečnosť preventívne stanovujú všeobecné a nediferencované uchovávanie údajov o prenose dát a polohe,

nebráni vnútroštátnym legislatívnym opatreniam, ktoré:

- **na účely ochrany národnej bezpečnosti umožňujú prikázať poskytovateľom elektronických komunikačných služieb, aby vykonali všeobecné a nediferencované uchovávanie údajov o prenose dát a polohe v situáciách, keď dotknutý členský štát čelí vážnej hrozbe pre národnú bezpečnosť, ktorá sa javí ako skutočná a aktuálna alebo predvídateľná, pričom rozhodnutie o vydaní takéhoto príkazu môže byť účinne preskúmané zo strany súdu alebo nezávislého správneho orgánu, ktorého rozhodnutie má záväzný účinok, a cieľom tohto preskúmania bude overiť existenciu jednej z týchto situácií a dodržanie podmienok a záruk, ktoré musia byť stanovené, a uvedený príkaz možno vydať len na časovo obmedzené obdobie, ktoré je striktne nevyhnutné, s možnosťou jeho predĺženia, pokiaľ takáto hrozba pretrváva,**
- **na účely ochrany národnej bezpečnosti, boja proti závažnej trestnej činnosti a predchádzania vážnym hrozbám pre verejnú bezpečnosť stanovujú ciele uchovávanie údajov o prenose dát a polohe, ktoré je vymedzené na základe objektívnych a nediskriminačných faktorov, podľa kategórií dotknutých osôb alebo prostredníctvom geografického kritéria, na časovo obmedzené obdobie, ktoré je striktne nevyhnutné, s možnosťou jeho predĺženia,**
- **na účely ochrany národnej bezpečnosti, boja proti závažnej trestnej činnosti a predchádzania vážnym hrozbám pre verejnú bezpečnosť stanovujú všeobecné a nediferencované uchovávanie IP adries pridelených zdroju spojenia na časovo obmedzené obdobie, ktoré je striktne nevyhnutné,**
- **na účely ochrany národnej bezpečnosti, boja proti trestnej činnosti a ochrany verejnej bezpečnosti stanovujú všeobecné a nediferencované uchovávanie údajov týkajúcich sa totožnosti užívateľov prostriedkov elektronickej komunikácie a**

- **na účely boja proti závažnej trestnej činnosti a *a fortiori* ochrany národnej bezpečnosti umožňujú prostredníctvom rozhodnutia príslušného orgánu, ktoré podlieha účinnému súdnemu preskúmaniu, prikázať poskytovateľom elektronických komunikačných služieb, aby urýchlene uchovali na potrebný čas údaje o prenose dát a polohe, ktoré majú k dispozícii,**

pokiaľ tieto opatrenia prostredníctvom jasných a presných pravidiel zabezpečujú, že uchovávanie dotknutých údajov podlieha dodržiavaniu príslušných hmotnoprávných a procesných podmienok a že dotknuté osoby majú účinné záruky proti rizikám zneužitia.

Podpisy