Zbierka súdnych rozhodnutí

NÁVRHY GENERÁLNEHO ADVOKÁTA
MANUEL CAMPOS SÁNCHEZ-BORDONA
prednesené 15. januára 2020 [1]

Spojené veci C-511/18 a C-512/18

La Quadrature du Net,
French Data Network,
Fédération des fournisseurs d'accès à Internet associatifs,
Igwan.net (C-511/18)
proti
Premier ministre,
Garde des Sceaux, ministre de la Justice,
Ministre de l'Intérieur,
Ministre des Armées

[návrh na začatie prejudiciálneho konania, ktorý podala Conseil d'État (Štátna rada, ktorá rozhoduje v postavení najvyššieho správneho súdu, Francúzsko)]

„Návrh na začatie prejudiciálneho konania – Spracovávanie osobných údajov a ochrana súkromia v sektore elektronických komunikácií – Ochrana národnej bezpečnosti a boj proti terorizmu – Smernica 2002/58/ES – Pôsobnosť – Článok 1 ods. 3 – Článok 15 ods. 3 – Článok 4 ods. 2 ZEÚ – Charta základných práv Európskej únie – Články 6, 7, 8, 11, 47 a článok 52 ods. 1 – Všeobecné a nediferencované uchovávanie údajov o pripojení a údajov, ktoré umožňujú identifikovať tvorcov obsahu – Zber údajov o prenose dát a polohe – Prístup k údajom"

1. Súdny dvor sa v posledných rokoch pridržiava ustálenej judikatúry týkajúcej sa uchovávania osobných údajov a prístupu k nim, ktorej hlavnými míľnikmi sú:

– rozsudok z 8. apríla 2014, Digital Rights Ireland a i. [2], v ktorom Súdny dvor vyhlásil smernicu 2006/24/ES [3] za neplatnú, lebo umožňovala neprimeraný zásah do práv uznaných v článkoch 7 a 8 Charty základných práv Európskej únie (ďalej len „Charta"),

– rozsudok z 21. decembra 2016, Tele2 Sverige a Watson a i. [4], v ktorom podal výklad článku 15 ods. 1 smernice 2002/58/ES [5],

– rozsudok z 2. októbra 2018, Ministerio Fiscal [6], v ktorom potvrdil výklad uvedeného ustanovenia smernice 2002/58.

1 Jazyk prednesu: španielčina.

2 Veci C-293/12 a C-594/12 (ďalej len „rozsudok Digital Rights", EU:C:2014:238).

3 Smernica Európskeho parlamentu a Rady 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).

4 Veci C-203/15 a C-698/15 (ďalej len „rozsudok Tele2 Sverige a Watson", EU:C:2016:970).

5 Smernica Európskeho parlamentu a Rady z 12. júla 2002 týkajúca sa spracovávania osobných údajov a ochrany súkromia v sektore elektronických komunikácií (smernica o súkromí a elektronických komunikáciách) (Ú. v. ES L 201, 2002, s. 37; Mim. vyd. 13/029, s. 514).

6 Vec C-207/16 (ďalej len „rozsudok Ministerio Fiscal", EU:C:2018:788).

2. Uvedené rozsudky (najmä druhý z nich) znepokojujú orgány niektorých členských štátov, lebo tieto orgány sa domnievajú, že uvedené rozsudky im odnímajú nástroj, ktorý považujú za nevyhnutný pre ochranu národnej bezpečnosti a pre boj proti trestnej činnosti a terorizmu. Preto niektoré z týchto členských štátov podporujú zrušenie alebo úpravu uvedenej judikatúry.

3. Určité súdy členských štátov poukázali na tú istú obavu v štyroch návrhoch na začatie prejudiciálneho konania[7], v súvislosti s ktorými prednášam návrhy v tento istý deň.

4. Tieto štyri veci vyvolávajú predovšetkým problém týkajúci sa uplatňovania smernice 2002/58 na činnosti súvisiace s národnou bezpečnosťou a bojom proti terorizmu. Ak by za týchto okolností platila uvedená smernica, bude následne potrebné objasniť, do akej miery môžu členské štáty obmedziť práva na súkromie, ktoré táto smernica chráni. Napokon bude potrebné preskúmať, do akej miery sú jednotlivé vnútroštátne právne úpravy (britská[8], belgická[9] a francúzska[10]) v tejto oblasti v súlade s právom Únie, ako ho vyložil Súdny dvor.

I. Právny rámec

A. Právo Únie

1. Smernica 2002/58

5. Podľa článku 1 („Rozsah platnosti a cieľ“):

„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 spracúvania osobných údajov v elektronickom komunikačnom sektore a zabezpečenia voľného pohybu takých údajov a elektronických komunikačných zariadení a služieb v Spoločenstve.

…

3. Táto smernica sa nevzťahuje na činnosti, ktoré sú mimo pôsobnosti zmluvy o založení Európskych spoločenstiev, ako sú činnosti podľa hlavy V a VI Zmluvy o Európskej únii[,] 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.“

6. Článok 3 („Dotknuté služby“) znie:

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

7 Okrem týchto dvoch vecí (veci C-511/18 a C-512/18) sú to veci C-623/17, Privacy International, a C-520/18, Ordre des barreaux francophones et germanophone a i.

8 Vec Privacy International, C-623/17.

9 Vec Ordre des barreaux francophones et germanophone a i., C-520/18.

10 Veci La Quadrature du Net a i., C-511/18 a C-512/18.

7. Článok 5 („Dôvernosť správy“) v odseku 1 stanovuje:

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

8. V článku 6 („Prevádzkové dáta [Údaje o prenose dát – *neoficiálny preklad*]“) sa uvádza:

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

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

9. Článok 15 („Uplatňovanie niektorých ustanovení smernice 95/46/ES[11]“) v odseku 1 stanovuje:

„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/ES. 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 Zmluvy o Európskej únii.“

2. Smernica 2000/31/ES[12]

10. Článok 14 znie:

„1. Ak sa poskytuje služba informačnej spoločnosti, ktorá pozostáva z uloženia informácií, ktoré sú poskytované príjemcom tejto služby, musia členské štáty zabezpečiť, aby poskytovateľ služby nebol zodpovedný za informácie uložené na žiadosť príjemcu služby, pod podmienkou, že:

…

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

12 Smernica Európskeho parlamentu a Rady z 8. júna 2000 o určitých právnych aspektoch služieb informačnej spoločnosti na vnútornom trhu, najmä o elektronickom obchode (smernica o elektronickom obchode) (Ú. v. ES L 178, 2000, s. 1; Mim. vyd. 13/025, s. 399).

3. Tento článok nemá vplyv na možnosť súdu alebo správneho orgánu požiadať poskytovateľa služieb, v súlade s právnymi systémami členských štátov, aby ukončil alebo predchádzal porušovaniu predpisov, a nemá vplyv ani na možnosť členských štátov, aby začali konanie, ktoré by nariadilo odstránenie alebo znemožnenie prístupu k informáciám.“

11. Podľa článku 15:

„1. Členské štáty neuložia poskytovateľom všeobecnú povinnosť pri poskytovaní služieb, na ktoré sa vzťahujú články 12, 13 a 14, aby monitorovali informácie, ktoré prenášajú alebo ktoré uložili, ani všeobecnú povinnosť aktívne zisťovať skutočnosti alebo okolnosti, ktoré by naznačovali, že ide o nezákonnú činnosť.

2. Členské štáty môžu ustanoviť povinnosť, aby poskytovatelia služieb informačnej spoločnosti informovali príslušné verejné orgány o údajných vykonávaných nezákonných činnostiach alebo o údajných nezákonných poskytovaných informáciách, alebo povinnosť oznamovať príslušným orgánom na ich žiadosť informácie, ktoré by im umožnili identifikáciu príjemcov ich služieb, s ktorými uzatvorili dohody o uložení informácií.“

3. Nariadenie (EÚ) 2016/679[13]

12. V súlade s článkom 2 („Vecná pôsobnosť“):

„1. Toto nariadenie sa vzťahuje na spracúvanie osobných údajov vykonávané úplne alebo čiastočne automatizovanými prostriedkami a na spracúvanie inými než automatizovanými prostriedkami v prípade osobných údajov, ktoré tvoria súčasť informačného systému alebo sú určené na to, aby tvorili súčasť informačného systému.

2. Toto nariadenie sa nevzťahuje na spracúvanie osobných údajov:

a) v rámci činnosti, ktorá nepatrí do pôsobnosti práva Únie;

b) členskými štátmi pri vykonávaní činností patriacich do rozsahu pôsobnosti kapitoly 2 hlavy V ZEÚ;

c) fyzickou osobou v rámci výlučne osobnej alebo domácej činnosti;

d) príslušnými orgánmi na účely predchádzania trestným činom, ich vyšetrovania, odhaľovania alebo stíhania, alebo výkonu trestných sankcií vrátane ochrany pred ohrozením verejnej bezpečnosti a jeho predchádzania.

…“

13 Nariadenie Európskeho parlamentu a Rady z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov) (Ú. v. EÚ L 119, 2016, s. 1).

13. Článok 23 („Obmedzenia“) v odseku 1 stanovuje:

„V práve Únie alebo práve členského štátu, ktorému prevádzkovateľ alebo sprostredkovateľ podliehajú, sa prostredníctvom legislatívneho opatrenia môže obmedziť rozsah povinností a práv ustanovených v článkoch 12 až 22 a v článku 34, ako aj v článku 5, pokiaľ jeho ustanovenia zodpovedajú právam a povinnostiam ustanoveným v článkoch 12 až 22, ak takéto obmedzenie rešpektuje podstatu základných práv a slobôd a je nevyhnutným a primeraným opatrením v demokratickej spoločnosti s cieľom zaistiť:

a) národnú bezpečnosť;

b) obranu;

c) verejnú bezpečnosť;

d) predchádzanie trestným činom, ich vyšetrovanie, odhaľovanie alebo stíhanie alebo výkon trestných sankcií vrátane ochrany pred ohrozením verejnej bezpečnosti a jeho predchádzanie;

e) iné dôležité ciele všeobecného verejného záujmu Únie alebo členského štátu, najmä predmet dôležitého hospodárskeho alebo finančného záujmu Únie alebo členského štátu vrátane peňažných, rozpočtových a daňových záležitostí, verejného zdravia a sociálneho zabezpečenia;

f) ochranu nezávislosti súdnictva a súdnych konaní;

g) predchádzanie porušeniam etiky pre regulované profesie, ich vyšetrovanie, odhaľovanie a stíhanie;

h) monitorovaciu, kontrolnú alebo regulačnú funkciu spojenú, hoci aj príležitostne, s výkonom verejnej moci v prípadoch uvedených v písmenách a) až e) a g);

i) ochranu dotknutej osoby alebo práv a slobôd iných;

j) vymáhanie občianskoprávnych nárokov.“

14. Článok 95 („Vzťah k smernici 2002/58/ES“) znie:

„Týmto nariadením sa fyzickým či právnickým osobám neukladajú dodatočné povinnosti, pokiaľ ide o spracúvanie v súvislosti s poskytovaním verejne dostupných elektronických komunikačných služieb vo verejných komunikačných sieťach v Únii, v prípadoch, keď podliehajú konkrétnym povinnostiam s rovnakým cieľom stanoveným v smernici 2002/58/ES.“

B. Vnútroštátne právo

1. Code de la sécurité intérieure (Zákonník vnútornej bezpečnosti)

15. V súlade s článkom L. 851-1:

„Za podmienok stanovených v kapitole 1 hlavy II tejto knihy možno povoliť, aby sa od prevádzkovateľov elektronických komunikácií a osôb uvedených v článku L. 34-1 code des postes et des communications électroniques [(Zákonník pôšt a elektronických komunikácií)], ako aj osôb uvedených v článku 6 ods. I bodoch 1 a 2 loi n.º 2004-575… pour la confiance dans l’économie numérique [(zákon č. 2004-575… o dôvere v digitálne hospodárstvo)] zbierali informácie alebo dokumenty spracúvané alebo uchovávané prostredníctvom ich elektronických komunikačných sietí

alebo služieb, vrátane technických údajov týkajúcich sa identifikácie čísiel predplatného alebo pripojenia k elektronickým komunikačným službám, identifikovania všetkých čísel predplatného alebo pripojenia určenej osoby, polohy používaných koncových zariadení, ako aj komunikácií účastníka týkajúcich sa zoznamu volaných a volajúcich čísel, trvania a dátumu komunikácie. …“

16. V článkoch L. 851-2 a L. 851-4 je – v závislosti od jednotlivých cieľov a pravidiel – upravený administratívny prístup k údajom o pripojení, ktoré sa takto uchovávajú, v reálnom čase.

17. Článok L. 851-2 povoľuje – iba na účely predchádzania terorizmu – zber informácií alebo dokumentov uvedených v článku L. 851-1 od tých istých osôb. Tento zber, ktorý sa týka len jedného alebo viacerých jednotlivcov vopred označených ako osoby, v prípade ktorých existuje podozrenie, že majú väzbu s teroristickou hrozbou, sa uskutočňuje v reálnom čase. To isté platí aj pre článok L. 851-4, ktorý dovoľuje, aby prevádzkovatelia v reálnom čase prenášali len technické údaje týkajúce sa polohy koncových zariadení. [14]

18. Článok L. 851-3 umožňuje uložiť prevádzkovateľom elektronických komunikácií a poskytovateľom technických služieb povinnosť týkajúcu sa „uplatňovania automatizovaných procesov spracovávania v ich sieťach na zisťovanie pripojení, ktoré by mohli predstavovať teroristickú hrozbu, v závislosti od parametrov určených v povolení“. [15]

19. Článok L. 851-5 spresňuje, že za určitých podmienok „možno povoliť použitie technického zariadenia, ktoré umožňuje v reálnom čase určiť polohu osoby, vozidla alebo veci“.

20. V súlade s článkom L. 851-6 ods. I je za určitých podmienok možné „prostredníctvom prístroja alebo technického zariadenia uvedeného v článku 226-3 bode 1 code pénal [(Trestný zákon)] priamo zbierať technické údaje o pripojení, ktoré umožňujú identifikáciu koncového zariadenia alebo účastníckeho čísla jeho používateľa, ako aj údaje o polohe použitých koncových zariadení“.

2. Zákonník pôšt a elektronických komunikácií

21. V zmysle článku L. 34-1 v znení uplatniteľnom na skutkový stav:

„I. Tento článok sa vzťahuje na spracovávanie osobných údajov pri poskytovaní elektronických komunikačných služieb verejnosti; vzťahuje sa najmä na siete, ktoré využívajú zariadenia na zber údajov a identifikačné zariadenia.

II. Bez toho, aby boli dotknuté odseky III, IV, V a VI, prevádzkovatelia elektronických komunikácií a najmä osoby, ktorých činnosť spočíva v poskytovaní prístupu verejnosti ku komunikačným službám online, vymažú alebo anonymizujú všetky údaje o prenose dát.

Osoby, ktoré poskytujú verejnosti elektronické komunikačné služby, zavedú v súlade s predchádzajúcim pododsekom interné postupy na spracovanie žiadostí príslušných orgánov.

Osoby, ktoré v rámci hlavnej alebo vedľajšej podnikateľskej činnosti poskytujú verejnosti pripojenie, ktoré umožňuje komunikáciu online prostredníctvom prístupu k sieti, a to aj bezodplatne, musia dodržiavať ustanovenia vzťahujúce sa na prevádzkovateľov elektronických komunikácií na základe tohto článku.

14 Podľa vnútroštátneho súdu tieto metódy neukladajú dotknutým poskytovateľom požiadavku dodatočného uchovávania v porovnaní s tým, čo je potrebné na fakturáciu ich služieb, uvádzanie týchto služieb na trh a poskytovanie služieb s pridanou hodnotou.

15 Podľa vnútroštátneho súdu táto metóda, ktorá nemá za následok všeobecné a nediferencované uchovávanie, má za cieľ vyzbierať počas obmedzenej doby spomedzi všetkých údajov o pripojení, ktoré tieto osoby spracovávajú, len tie údaje, ktoré by mohli súvisieť s takýmto závažným trestným činom.

III. Na účely vyšetrovania, odhaľovania a stíhania trestných činov alebo porušenia povinnosti vymedzenej v článku L. 336-3 code de la propriété intellectuelle [(Zákonník duševného vlastníctva)] alebo na účely predchádzania útokom na systémy automatizovaného spracovávania údajov stanoveným a sankcionovaným v článkoch 323-1 až 323-3-1 Trestného zákona a len s cieľom umožniť v prípade potreby poskytnutie súdnemu orgánu alebo vysokému orgánu uvedenému v článku L. 331-12 Zákonníka duševného vlastníctva alebo národnému orgánu pre bezpečnosť informačných systémov uvedenému v článku L. 2321-1 code de la défense [(Obranný zákonník)] možno úkony zamerané na vymazanie alebo anonymizáciu určitých kategórií technických údajov odložiť najdlhšie o jeden rok. Dekrétom prerokovaným v Conseil d'État [(Štátna rada)], prijatým po stanovisku Commission nationale de l'informatique et des libertés [(Národná komisia pre informačné technológie a občianske slobody)], sa v medziach stanovených v odseku VI určia tieto kategórie údajov a doba ich uchovávania podľa činnosti prevádzkovateľov a povahy komunikácie, ako aj podmienky náhrady prípadných dodatočných nákladov, ktoré možno určiť a ktoré konkrétne súvisia so službami, ktoré prevádzkovatelia z tohto dôvodu zabezpečujú na žiadosť štátu.

…

VI. Údaje uchovávané a spracovávané za podmienok stanovených v odsekoch III, IV a V sa týkajú výlučne identifikácie užívateľov služieb poskytovaných prevádzkovateľmi, technických vlastností komunikácie zabezpečovanej prevádzkovateľmi a polohy koncových zariadení.

V nijakom prípade sa nemôžu týkať obsahu prijatej alebo odoslanej korešpondencie alebo informácií konzultovaných v akejkoľvek forme v rámci tejto komunikácie.

Uchovávanie a spracovávanie údajov sa uskutočňuje v súlade s ustanoveniami zákona č. 78-17 zo 6. januára 1978 o informatike, súboroch a slobodách.

Prevádzkovatelia prijmú všetky opatrenia s cieľom zabrániť využívaniu týchto údajov na iné účely než tie, ktoré sú uvedené v tomto článku."

22. Na základe článku R. 10-13 ods. I musia prevádzkovatelia na účely vyšetrovania, odhaľovania a stíhania trestných činov uchovávať nasledujúce údaje:

„a) informácie, ktoré umožňujú identifikovať užívateľa;

b) údaje o použitých koncových komunikačných zariadeniach;

c) technické vlastnosti, ako aj dátum, čas a dĺžku trvania každej komunikácie;

d) údaje o vyžiadaných alebo použitých doplnkových službách a ich poskytovateľoch;

e) údaje, ktoré umožňujú identifikovať jedného alebo viacerých adresátov komunikácie."

23. Podľa odseku II toho istého ustanovenia v prípade telefonických činností musí prevádzkovateľ navyše uchovávať údaje, ktoré umožnia identifikovať pôvod a polohu komunikácie.

24. V súlade s odsekom III toho istého článku sa spomenuté údaje musia uchovávať jeden rok odo dňa ich zaznamenania.

3. Loi n.º 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (zákon č. 2004-575 z 21. júna 2004 o dôvere v digitálne hospodárstvo)

25. Článok 6 ods. II prvý pododsek la zákona č. 2004-575 stanovuje, že osoby, ktorých činnosť spočíva v poskytovaní prístupu verejnosti ku komunikačným službám online, a fyzické alebo právnické osoby, ktoré na účely poskytovania verejnosti prostredníctvom verejných komunikačných služieb online, a to aj bezodplatne, zabezpečujú uchovávanie signálov, písaného textu, obrázkov a zvukov alebo správ akéhokoľvek druhu dodaných príjemcami týchto služieb, „ukladajú a uchovávajú údaje tak, aby bolo možné zistiť, kto prispel k tvorbe obsahu alebo jedného z obsahov služieb, ktorých sú poskytovateľmi".

26. V treťom pododseku odseku II toho istého ustanovenia sa uvádza, že súdny orgán môže od týchto osôb vyžadovať poskytnutie údajov uvedených v prvom pododseku.

27. Podľa posledného pododseku odseku II dekrétom Conseil d'État (Štátna rada) „sa určia údaje uvedené v prvom pododseku a stanoví sa doba a podmienky ich uchovávania".[16]

II. Skutkový stav a položené prejudiciálne otázky

A. Vec C-511/18

28. La Quadrature du Net, French Data Network, Igwan.net a Fédération des fournisseurs d'accès à Internet associatifs (ďalej len „žalobcovia") navrhli, aby Conseil d'État (Štátna rada) zrušila viaceré dekréty, ktorými sa vykonávajú niektoré ustanovenia Zákonníka vnútornej bezpečnosti.[17]

29. Žalobcovia v podstate tvrdili, že tak napadnuté dekréty, ako aj uvedené ustanovenia Zákonníka vnútornej bezpečnosti porušujú právo na rešpektovanie súkromného života, právo na ochranu osobných údajov a právo na účinný prostriedok nápravy zaručené v článkoch 7, 8 a 47 Charty.

16 Tieto údaje boli určené prostredníctvom décret n.º 2011-219 du 25 février 2011 relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne (dekrét č. 2011-219 z 25. februára 2011 o uchovávaní a poskytovaní údajov, ktoré umožňujú identifikovať každú osobu, ktorá prispela k vytvoreniu obsahu poskytovaného online). Spomedzi ustanovení tohto dekrétu možno poukázať na: a) článok 1 ods. 1, podľa ktorého osoby, ktoré poskytujú prístup ku komunikačným službám online, musia uchovávať tieto údaje: identifikátor pripojenia, identifikátor priradený účastníkovi, identifikátor koncového zariadenia použitého pri pripojení, dátum a čas začatia a ukončenia pripojenia, vlastnosti linky účastníka; b) podľa článku 1 ods. 2 osoby, ktoré na účely poskytovania verejnosti prostredníctvom verejných komunikačných služieb online, a to aj bezodplatne, zabezpečujú uchovávanie signálov, písaného textu, obrázkov a zvukov alebo správ akéhokoľvek druhu dodaných príjemcami týchto služieb, musia v prípade každej operácie uchovávať tieto údaje: identifikátor pripojenia na začiatku komunikácie, identifikátor priradený obsahu, ktorý je predmetom operácie, typy protokolov použitých na pripojenie k službe a na prenos obsahu, povaha operácie, dátum a čas operácie, identifikátor použitý autorom operácie a c) napokon článok 1 ods. 3 stanovuje, že osoby spomenuté v oboch vyššie uvedených odsekoch musia uchovávať nasledujúce informácie, ktoré užívateľ poskytol pri uzatvorení zmluvy alebo vytvorení účtu: identifikátor pripojenia v čase vytvorenia účtu; meno, priezvisko alebo obchodné meno; súvisiace poštové adresy, použité aliasy, súvisiace e-mailové adresy a adresy účtu, telefónne čísla, aktuálne heslo a údaje, ktoré ho umožňujú overiť alebo zmeniť.

17 Napadnutými dekrétmi boli: a) décret n.º 2015-1885 du 28 septembre 2015 portant désignation des services spécialisés de renseignement (dekrét č. 2015-1185 z 28. septembra 2015 o určovaní špecializovaných spravodajských služieb); b) décret n.º 2015-1211 du 1er octubre 2015 relatif au contentieux de la mise en oeuvre des techniques de renseignement soumises à autorisation et des fichiers intéressant la sûreté de l'État (dekrét č. 2015-1211 z 1. októbra 2015 o súdnych konaniach týkajúcich sa uplatňovania spravodajských metód, ktoré podliehajú povoleniu, a záznamov týkajúcich sa bezpečnosti štátu); c) décret n.º 2015-1639 du 11 décembre 2015 relatif à la désignation des services autres que les services spécialisés de renseignement, autorisés à recourir aux techniques mentionnées au titre V du libre VIII du code de la sécurité intérieure (dekrét č. 2015-1639 z 11. decembra 2015 o určovaní služieb, ktoré nie sú špecializovanými spravodajskými službami, oprávnených využívať metódy uvedené v hlave V knihy VIII Zákonníka vnútornej bezpečnosti), a d) décret n.º 2016-67 du 29 janvier 2016 relatif aux techniques de recueil de renseignement (dekrét č. 2016-67 z 29. januára 2016 o metódach získavania informácií).

30. Za týchto okolností Conseil d'État (Štátna rada) kladie Súdnemu dvoru nasledujúce otázky:

„1. Má sa povinnosť všeobecného a nediferencovaného uchovávania, uložená poskytovateľom na základe ustanovení článku 15 ods. 1 [smernice 2002/58], považovať v kontexte, ktorý sa vyznačuje vážnymi a pretrvávajúcimi hrozbami pre národnú bezpečnosť, najmä rizikom terorizmu, za zásah odôvodnený právom na bezpečnosť zaručeným v článku 6 Charty… a požiadavkami národnej bezpečnosti, za ktorú podľa článku 4 [ZEÚ] nesú zodpovednosť len členské štáty?

2. Má sa [smernica 2002/58], v spojení s Chartou…, vykladať v tom zmysle, že povoľuje legislatívne opatrenia, akými sú opatrenia týkajúce sa zberu údajov o prenose dát a polohe určitých jednotlivcov v reálnom čase, ktoré síce zasahujú do práv a povinností poskytovateľov elektronických komunikačných služieb, no neukladajú im konkrétnu povinnosť uchovávať ich údaje?

3. Má sa [smernica 2002/58], v spojení s Chartou…, vykladať v tom zmysle, že v každom prípade podmieňuje zákonnosť postupov zberu údajov o pripojení požiadavkou informovania dotknutých osôb, pokiaľ takáto informácia už nemôže ohroziť vyšetrovanie vedené príslušnými orgánmi, alebo takéto postupy sa môžu považovať za zákonné vzhľadom na všetky ostatné existujúce procesné záruky za predpokladu, že tieto záruky zabezpečujú účinnosť práva na prostriedok nápravy?“

B. Vec C-512/18

31. Žalobcovia v konaní, v ktorom bol podaný návrh na začatie prejudiciálneho konania vo veci C-511/18, s výnimkou združenia Igwan.net, tiež navrhli, aby Conseil d'État (Štátna rada) zrušila rozhodnutie o zamietnutí (v dôsledku nečinnosti správneho orgánu) ich žiadosti o zrušenie článku R. 10-13 code des postes et des communications électroniques (Zákonník pôšt a elektronických komunikácií) a dekrétu č. 2011-219 z 25. februára 2011.

32. Podľa názoru uvedených žalobcov napadnuté predpisy ukladajú povinnosť uchovávať údajov o prenose dát, polohe a pripojení, ktorá vzhľadom na svoj všeobecný charakter prestavuje neprimeraný zásah do práva na rešpektovanie súkromného a rodinného života, práva na ochranu osobných údajov a práva na slobodu prejavu, ktoré sú chránené článkami 7, 8 a 11 Charty, ktorý je v rozpore s článkom 15 ods. 1 smernice 2002/58.

33. V uvedenom konaní Conseil d'État (Štátna rada) položila tieto prejudiciálne otázky:

„1. Má sa povinnosť všeobecného a nediferencovaného uchovávania, uložená poskytovateľom na základe ustanovení článku 15 ods. 1 [smernice 2002/58], považovať najmä vzhľadom na záruky a kontroly, ktoré sú spojené so zberom a použitím týchto údajov o pripojení, za zásah odôvodnený právom na bezpečnosť zaručeným v článku 6 Charty… a požiadavkami národnej bezpečnosti, za ktorú podľa článku 4 [ZEÚ] nesú zodpovednosť len členské štáty?

2. Majú sa ustanovenia [smernice 2000/31], v spojení s článkami 6, 7, 8 a 11, ako aj článkom 52 ods. 1 Charty…, vykladať v tom zmysle, že umožňujú členskému štátu zaviesť vnútroštátnu právnu úpravu, ktorá ukladá osobám, ktorých činnosť spočíva v poskytovaní prístupu verejnosti ku komunikačným službám online, a fyzickým alebo právnickým osobám, ktoré na účely poskytovania verejnosti prostredníctvom verejných komunikačných služieb online, a to aj bezodplatne, zabezpečujú uchovávanie signálov, písaného textu, obrázkov a zvukov alebo správ akéhokoľvek druhu dodaných príjemcami týchto služieb, povinnosť uchovávať údaje umožňujúce zistiť, kto prispel k tvorbe obsahu alebo jedného z obsahov služieb, ktorých sú poskytovateľmi, aby súdny orgán mohol prípadne požiadať o ich poskytnutie na účely uplatňovania predpisov týkajúcich sa občianskoprávnej alebo trestnej zodpovednosti?“

III. Konanie na Súdnom dvore a stanoviská účastníkov konania

34. Návrhy na začatie prejudiciálneho konania boli doručené do kancelárie Súdneho dvora 3. augusta 2018.

35. Písomné pripomienky predložili La Quadrature du Net, Fédération des fournisseurs d'accès à Internet associatifs, French Data Network, nemecká, belgická, britská, česká, cyperská, dánska, španielska, estónska, francúzska, maďarská, írska, poľská a švédska vláda, ako aj Komisia.

36. Dňa 9. septembra 2019 sa uskutočnilo pojednávanie, ktoré sa konalo spoločne s pojednávaniami vo veciach C-623/17, Privacy International, a C-520/18, Ordre des barreaux francophones et germanophone a i., a na ktorom boli zastúpení účastníci všetkých štyroch konaní, v ktorých boli podané návrhy na začatie prejudiciálneho konania, vyššie uvedené vlády, holandská a nórska vláda, ako aj Komisia a Európsky dozorný úradník pre ochranu údajov.

IV. Analýza

37. Otázky, ktoré položila Conseil d'État (Štátna rada), možno rozdeliť na tri otázky:

– v prvom rade, či je s právom Únie zlučiteľná vnútroštátna právna úprava, ktorá ukladá poskytovateľom elektronických komunikačných služieb povinnosť všeobecne a nediferencovane uchovávať údaje o pripojení (prvá otázka vo veci C-511/18 a vo veci C-512/18) a najmä údaje, ktoré umožňujú identifikovať tvorcov obsahov ponúkaných týmito poskytovateľmi (druhá otázka vo veci C-512/18),

– v druhom rade, či je zákonnosť postupov zberu údajov o pripojení v každom prípade podmienená povinnosťou informovať dotknuté osoby, ak to neohrozí vyšetrovanie (tretia otázka vo veci C-511/18),

– v treťom rade, či a za akých podmienok je zber údajov o prenose dát a polohe v reálnom čase bez povinnosti uchovávať ich zlučiteľný so smernicou 2002/58 (druhá otázka vo veci C-511/18).

38. V konečnom dôsledku je potrebné určiť, či je v súlade s právom Únie vnútroštátna právna úprava, ktorá ukladá poskytovateľom elektronických komunikačných služieb dva druhy povinností: a) na jednej strane povinnosť *zbierať* určité údaje, no nie uchovávať ich, a b) na druhej strane povinnosť *uchovávať* údaje o pripojení a údaje, ktoré umožňujú identifikovať tvorcov obsahov služieb poskytovaných takými poskytovateľmi.

39. Najprv treba rozhodnúť, či sa – práve z dôvodu kontextu [18], v ktorom bola uvedená vnútroštátna právna úprava prijatá (teda za okolností, za ktorých môže byť ohrozená národná bezpečnosť) – uplatní smernica 2002/58.

A. O uplatniteľnosti smernice 2002/58

40. Vnútroštátny súd vychádza z predpokladu, že právna úprava, ktorá je predmetom sporu, spadá do pôsobnosti smernice 2002/58. Podľa jeho názoru to vyplýva z judikatúry stanovenej v rozsudku Tele2 Sverige a Watson a potvrdenej v rozsudku Ministerio Fiscal.

18 Ako je spresnené v prvej otázke vo veci C-511/18, ide o „kontex[t], ktorý sa vyznačuje vážnymi a pretrvávajúcimi hrozbami pre národnú bezpečnosť, najmä rizikom terorizmu".

41. Naopak niektoré z vlád, ktoré vstúpili do konania, tvrdia, že sporná právna úprava nepatrí do pôsobnosti uvedenej smernice. Na podporu svojho stanoviska uvádzajú okrem iných tvrdení rozsudok z 30. mája 2006, Parlament/Rada a Komisia [19].

42. Súhlasím s Conseil d'État (Štátna rada) v tom, že rozsudkom Tele 2 Sverige a Watson sa vyriešila táto časť diskusie, pričom sa potvrdilo, že smernica 2002/58 sa uplatňuje v zásade vtedy, keď poskytovatelia elektronických služieb sú podľa zákona povinní uchovávať údaje o svojich účastníkoch a poskytnúť orgánom verejnej moci prístup k nim. Na tomto názore nič nemení skutočnosť, že poskytovateľom sa ukladajú povinnosti z dôvodov národnej bezpečnosti.

43. Už teraz musím uviesť, že ak by existoval nejaký rozpor medzi rozsudkom Tele 2 Sverige a Watson a predchádzajúcimi rozsudkami, mal by sa uprednostniť prvý uvedený rozsudok, keďže bol vydaný neskôr a bol opäť potvrdený rozsudkom Ministerio Fiscal. Domnievam sa však, že uvedený rozpor neexistuje, čo sa pokúsim vysvetliť.

1. Rozsudok Parlament/Rada a Komisia

44. Veci, o ktorých sa rozhodlo rozsudkom Parlament/Rada a Komisia, sa týkali:

– dohody medzi Európskym spoločenstvom a Spojenými štátmi americkými o spracovaní a postúpení údajov PNR [Passenger Name Records (záznamy o cestujúcich)] leteckými dopravcami orgánom Spojených štátov amerických, [20]

– primeranosti ochrany osobných údajov obsiahnutých v záznamoch o cestujúcich lietadlom poskytovaných uvedeným orgánom. [21]

45. Súdny dvor dospel k záveru, že prenos týchto údajov predstavuje spracovanie, ktorého cieľom je verejná bezpečnosť a štátne činnosti týkajúce sa oblasti trestného práva. V súlade s článkom 3 ods. 2 prvou zarážkou smernice 95/46 obidve sporné rozhodnutia nepatrili do pôsobnosti smernice 95/46.

46. Letecké spoločnosti najprv zbierali údaje v rámci činnosti – predaj leteniek – patriacej do pôsobnosti práva Únie. Ich spracovanie, ako bolo upravené v spornom rozhodnutí, však nebolo „nevyhnutn[é] na poskytnutie služby, ale sa považ[ovalo] za nevyhnutné na zabezpečenie verejnej bezpečnosti a na represívne účely“. [22]

19 Veci C-317/04 a C-318/04 (ďalej len „rozsudok Parlament/Rada a Komisia“, EU:C:2006:346).

20 Rozhodnutie Rady 2004/496/ES zo 17. mája 2004 o uzavretí dohody medzi Európskym spoločenstvom a Spojenými štátmi americkými o spracovaní a postúpení údajov PNR leteckými dopravcami Úradu pre colnú správu a ochranu hraníc [Úradu colnej správy a ochrany hraníc – *neoficiálny preklad*] Ministerstva vnútornej bezpečnosti Spojených štátov amerických (Ú. v. EÚ L 183, 2004, s. 83) (vec C-317/04).

21 Rozhodnutie Komisie 2004/535/ES zo 14. mája 2004 o adekvátnej ochrane osobných údajov uvedených v Zázname podľa mena cestujúceho o cestujúcich lietadlom odoslaných Úradu Spojených štátov na ochranu colného priestoru a hraníc [o primeranej úrovni ochrany osobných údajov uvedených v záznamoch o cestujúcich lietadlom poskytnutých Úradu colnej správy a ochrany hraníc Spojených štátov amerických – *neoficiálny preklad*] (Ú. v. EÚ L 235, 2004, s. 11) (vec C-318/04).

22 Rozsudok Parlament/Rada a Komisia, bod 57. V bode 58 sa zdôrazňuje, že skutočnosť, že „údaje… zhromaždili súkromní podnikatelia na komerčné účely a že títo podnikatelia zabezpečujú ich prenos do tretej krajiny“, neznamená, že tento prenos nepredstavuje jeden z prípadov neuplatnenia smernice 95/46 vymenovaných v článku 3 ods. 2 prvej zarážke tejto smernice, lebo „tento prenos… patrí do rámca vytvoreného orgánmi verejnej moci na účely verejnej bezpečnosti“.

47. Súdny dvor teda použil teleologický prístup, pričom vychádzal z cieľa, ktorý sa mal spracovávaním údajov dosiahnuť: keďže jeho cieľom bola ochrana verejnej bezpečnosti, toto spracovávanie sa malo považovať za vyňaté z pôsobnosti smernice 95/46. Uvedený cieľ však nebol jediným rozhodujúcim kritériom [23], a preto bolo v tomto rozsudku zdôraznené, že toto spracovávanie „patrí do rámca vytvoreného orgánmi verejnej moci na účely verejnej bezpečnosti“. [24]

48. Rozsudok Parlament/Rada a Komisia teda objasňuje rozdiel medzi ustanovením o vylúčení a ustanoveniami o obmedzení, ktoré sú súčasťou smernice 95/46 (podobnými ustanoveniam smernice 2002/58). Je však pravda, že obe kategórie ustanovení sa týkajú podobných cieľov všeobecného záujmu, čo vyvoláva určité nejasnosti týkajúce sa ich pôsobnosti, ako už skôr poznamenal generálny advokát Bot. [25]

49. Je pravdepodobné, že z týchto nejasností pramení stanovisko, ktoré zastávajú členské štáty, ktoré tvrdia, že smernica 2002/58 sa za týchto okolností neuplatní. Podľa ich názoru je záujem národnej bezpečnosti chránený len prostredníctvom vylúčenia stanoveného v článku 1 ods. 3 smernice 2002/58. Nemožno však pochybovať o tom, že tomuto záujmu slúžia aj obmedzenia povolené článkom 15 ods. 1 uvedenej smernice, ku ktorým patrí obmedzenie týkajúce sa národnej bezpečnosti. Toto posledné uvedené ustanovenie by bolo nadbytočné, ak by sa smernica 2002/58 v prípade akéhokoľvek odvolania sa na národnú bezpečnosť neuplatnila.

2. Rozsudok Tele2 Sverige a Watson

50. Predmetom rozsudku Tele2 Sverige a Watson bola otázka zlučiteľnosti niektorých vnútroštátnych právnych úprav, ktoré ukladali poskytovateľom verejne dostupných elektronických komunikačných služieb všeobecnú povinnosť uchovávať údaje o elektronických komunikáciách, s právom Únie. Posudzované prípady boli preto v podstate totožné s prípadmi, o ktorých sa rozhoduje v týchto prejudiciálnych konaniach.

51. Súdny dvor, ktorý mal opäť posúdiť uplatniteľnosť práva Únie – tento raz už za účinnosti smernice 2002/58 –, najprv uviedol, že „rozsah pôsobnosti smernice 2002/58 treba posúdiť so zreteľom najmä na všeobecnú systematiku tejto smernice“. [26]

52. Z uvedeného hľadiska Súdny dvor poznamenal, že „je isté, že legislatívne opatrenia uvedené v článku 15 ods. 1 smernice 2002/58 predstavujú činnosti štátu alebo štátnych orgánov a nepatria do oblasti činností jednotlivcov… Okrem toho účely, ktoré musia podľa tohto ustanovenia tieto opatrenia spĺňať – v predmetnom prípade ochrana národnej bezpečnosti… – sa výrazne prekrývajú s cieľmi sledovanými činnosťami uvedenými v článku 1 ods. 3 tejto smernice“. [27]

23 Generálny advokát Bot, ktorý žiaľ už nie je medzi nami, na to v minulosti poukázal v návrhoch, ktoré predniesol vo veci Írsko/Parlament a Rada (C-301/06, EU:C:2008:558). Uviedol, že z rozsudku Parlament/Rada a Komisia „nevyplýva, že na účely zahrnutia alebo vylúčenia spracovania do pôsobnosti alebo z pôsobnosti systému ochrany údajov zavedeného smernicou 95/46 je relevantné len skúmanie cieľa, ktorý také spracovanie údajov sleduje. Treba tiež určiť, počas akej činnosti sa spracovanie údajov vykonáva. Je to tak len vtedy, pokiaľ sa spracovanie uskutočňuje v priebehu činností, ktoré sú vlastné štátu a štátnym orgánom a nepatria do oblasti činností jednotlivcov, ktorá je vylúčená zo systému ochrany osobných údajov Spoločenstva zavedeného článkom 3 ods. 2 prvou zarážkou smernice 95/46 [Spracovanie je vylúčené zo systému ochrany osobných údajov Spoločenstva zavedeného smernicou 95/46 len vtedy, ak sa uskutočňuje v priebehu činností, ktoré sú vlastné štátu a štátnym orgánom a nepatria do oblasti činností jednotlivcov, a to na základe článku 3 ods. 2 prvej zarážky tejto smernice – *neoficiálny preklad*]“ (bod 122).

24 Rozsudok Parlament/Rada a Komisia, bod 58. Hlavným cieľom tejto dohody bolo vyžadovať od leteckých dopravcov, ktorí prevádzkovali osobnú leteckú prepravu medzi Úniou a Spojenými štátmi americkými, aby poskytovali orgánom Spojených štátov amerických elektronický prístup k údajom PNR uvedeným v záznamoch o cestujúcich, ktoré sa nachádzali v ich počítačových systémoch na kontrolu rezervácií a odletov. Táto dohoda teda zavádzala určitú formu medzinárodnej spolupráce medzi Úniou a Spojenými štátmi americkými na účely boja proti terorizmu a iným závažným trestným činom, pričom sa pokúšala zosúladiť uvedený cieľ s cieľom ochrany osobných údajov cestujúcich. Za týchto okolností sa povinnosť uložená leteckým dopravcom veľmi neodlišovala od priamej výmeny údajov medzi orgánmi verejnej moci.

25 Návrhy, ktoré predniesol generálny advokát Bot vo veci Írsko/Parlament a Rada (C-301/06, EU:C:2008:558, bod 127).

26 Rozsudok Tele2 Sverige a Watson, bod 67.

27 Tamže, bod 72.

53. Účel opatrení, ktoré v súlade s článkom 15 ods. 1 smernice 2002/58 môžu prijať členské štáty na obmedzenie práva na súkromie, sa teda (v tomto bode) zhoduje s účelom, ktorý v súlade s článkom 1 ods. 3 tejto smernice odôvodňuje vylúčenie určitých štátnych činností z jej pôsobnosti.

54. Súdny dvor sa však domnieval, že „vzhľadom na všeobecnú systematiku smernice 2002/58“ na základe uvedenej skutočnosti nebolo možné „dospieť k záveru, že legislatívne opatrenia uvedené v článku 15 ods. 1 smernice 2002/58 sú vyňaté z pôsobnosti tejto smernice, pretože inak by bolo toto ustanovenie zbavené všetkého potrebného účinku. Dané ustanovenie totiž nevyhnutne predpokladá, že vnútroštátne opatrenia, ktoré sú v ňom uvedené…, spadajú do rozsahu pôsobnosti tejto smernice, pretože táto smernica výslovne dovoľuje členským štátom prijať také opatrenia len za určitých podmienok, ktoré sú v nej stanovené“. [28]

55. Okrem toho, čo bolo uvedené vyššie, obmedzenia povolené článkom 15 ods. 1 smernice 2002/58 „upravujú na účely uvedené v tomto ustanovení činnosť poskytovateľov elektronických komunikačných služieb“. Preto sa má uvedené ustanovenie v spojení s článkom 3 tejto smernice „vykladať v tom zmysle, že takéto legislatívne opatrenia spadajú do pôsobnosti tejto smernice“. [29]

56. Súdny dvor v dôsledku toho uviedol, že do pôsobnosti smernice 2002/58 spadá tak legislatívne opatrenie, ktoré ukladá poskytovateľom „povinnosť uchovávať údaje o prenose dát a polohe, pretože takáto činnosť nevyhnutne znamená spracúvanie osobných údajov týmito poskytovateľmi“, [30] ako aj legislatívne opatrenie, ktoré sa týka prístupu orgánov k údajom uchovávaným týmito poskytovateľmi [31].

57. Výklad smernice 2002/58, ktorý Súdny dvor podal v rozsudku Tele2 Sverige a Watson, bol zopakovaný v rozsudku Ministerio Fiscal.

58. Bolo by možné tvrdiť, že rozsudok Tele2 Sverige a Watson predstavuje – viac či menej implicitný – obrat oproti judikatúre stanovenej v rozsudku Parlament/Rada a Komisia? Tento názor zastáva napríklad írska vláda, podľa ktorej je len tento posledný uvedený rozsudok zlučiteľný s právnym základom smernice 2002/58 a v súlade s článkom 4 ods. 2 ZEÚ. [32]

59. Francúzska vláda sa zasa domnieva, že tento rozpor možno prekonať, ak sa vezme do úvahy skutočnosť, že judikatúra stanovená v rozsudku Tele2 Sverige a Watson sa týka činností členských štátov v oblasti trestného práva, zatiaľ čo judikatúra stanovená v rozsudku Parlament/Rada a Komisia súvisí s bezpečnosťou štátu a obranou. Judikatúra vyplývajúca z rozsudku Tele2 Sverige a Watson by sa teda nevzťahovala na prejednávaný prípad, v ktorom by sa muselo ešte stále uplatniť riešenie použité v rozsudku Parlament/Rada a Komisia. [33]

60. Ako som už uviedol, domnievam sa, že sa dá nájsť spôsob, ako zosúladiť oba rozsudky, iný než ten, ktorý podporuje francúzska vláda. Nesúhlasím s týmto spôsobom, lebo podľa môjho názoru úvahy uvedené v rozsudku Tele2 Sverige a Watson, ktoré sa výslovne týkajú boja proti terorizmu [34], možno rozšíriť na akúkoľvek inú hrozbu pre národnú bezpečnosť (pričom terorizmus je len jednou z takých hrozieb).

28 Tamže, bod 73.

29 Tamže, bod 74.

30 Tamže, bod 75.

31 Tamže, bod 76.

32 Body 15 a 16 písomných pripomienok írskej vlády.

33 Body 34 až 50 písomných pripomienok francúzskej vlády.

34 Rozsudok Tele2 Sverige a Watson, body 103 a 119.

3. Možnosť vyložiť rozsudok Parlament/Rada a Komisia v súlade s rozsudkom Tele2 Sverige a Watson

61. Podľa môjho názoru Súdny dvor v rozsudku Tele2 Sverige a Watson a v rozsudku Ministerio Fiscal vzal do úvahy dôvod existencie ustanovení o vylúčení a obmedzení, ako aj systémový vzťah medzi týmito dvoma druhmi ustanovení.

62. Ak Súdny dvor vo veci Parlament/Rada a Komisia konštatoval, že spracovanie údajov nepatrí do pôsobnosti smernice 95/46, urobil to – ako som už pripomenul – z dôvodu, že v kontexte spolupráce medzi Európskou úniou a Spojenými štátmi americkými v typicky medzinárodnom rámci musel mať prednosť štátny rozmer činnosti pred skutočnosťou, že toto spracovanie malo aj obchodný alebo súkromný rozmer. Jednou z otázok, o ktorých sa vtedy diskutovalo, bol práve vhodný právny základ na prijatie sporného rozhodnutia.

63. Pokiaľ ide vnútroštátne opatrenia skúmané v rozsudku Tele2 Sverige a Watson a v rozsudku Ministerio Fiscal, Súdny dvor naopak postavil do popredia vnútroštátny dosah spracovávania údajov: právny rámec, v ktorom k spracovávaniu údajov dochádzalo, bol výlučne vnútroštátny, a preto nemal zahraničný rozmer, ktorým sa vyznačoval predmet rozsudku Parlament/Rada a Komisia.

64. Rozdielny význam medzinárodného a vnútroštátneho (obchodného a súkromného) rozmeru spracovávania údajov mal za následok, že v prvom uvedenom prípade sa muselo použiť ustanovenie o vylúčení z pôsobnosti práva Únie ako najvhodnejšie ustanovenie na zabezpečenie ochrany všeobecného záujmu spočívajúceho v národnej bezpečnosti. V druhom uvedenom prípade sa ten istý záujem mohol účinne zohľadniť prostredníctvom ustanovenia o obmedzení obsiahnutého v článku 15 ods. 1 smernice 2002/58.

65. Možno ešte poukázať na ďalší rozdiel, ktorý súvisí s odlišným normatívnym kontextom: každý z týchto rozsudkov sa zameral na výklad dvoch ustanovení, ktoré nie sú rovnaké, aj keď sa to na prvý pohľad zdá.

66. Súdny dvor sa totiž v rozsudku Parlament/Rada a Komisia vyjadril k výkladu článku 3 ods. 2 smernice 95/46, zatiaľ čo v rozsudku Tele2 Sverige a Watson sa vyjadril k článku 1 ods. 3 smernice 2002/58. Z dôkladného preskúmania znenia týchto článkov vyplýva rozdiel, ktorý postačuje na podloženie zmyslu rozhodnutí Súdneho dvora v jednom aj v druhom prípade.

67. V súlade s článkom 3 ods. 2 smernice 95/46 „táto smernica *sa neuplatňuje na spracovanie osobných údajov*… v priebehu činností, ktoré sú mimo rozsahu zákona spoločenstva [mimo pôsobnosti práva Spoločenstva – *neoficiálny preklad*]…, a v žiadnom prípade sa neuplatňujú [neuplatňuje – *neoficiálny preklad*] 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 [trestného práva – *neoficiálny preklad*]“.[35]

68. Podľa článku 1 ods. 3 smernice 2002/58 sa táto smernica „*nevzťahuje na činnosti*, ktoré sú mimo pôsobnosti zmluvy o založení Európskych spoločenstiev,… 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 [štátu] v oblasti trestného práva“.[36]

35 Kurzívou zvýraznil generálny advokát.

36 Kurzívou zvýraznil generálny advokát.

69. Zatiaľ čo článok 3 ods. 2 smernice 95/46 vylučuje *operácie spracovania*, ktoré sa týkajú – v rozsahu relevantnom pre prejednávaný prípad – bezpečnosti štátu, článok 1 ods. 3 smernice 2002/58 vylučuje *činnosti* zamerané na ochranu – tiež v rozsahu relevantnom pre prejednávaný prípad – bezpečnosti štátu.

70. Tento rozdiel nie je zanedbateľný. Smernica 95/46 stanovovala, že z jej pôsobnosti je vylúčená činnosť („spracovanie osobných údajov"), ktorú môže vykonávať ktokoľvek. Z tejto činnosti boli osobitne vyňaté operácie spracovania, ktoré sa týkali okrem iného bezpečnosti štátu. Povaha *subjektu*, ktorý vykonával spracovanie údajov, bola naopak nepodstatná. Prístup použitý na identifikáciu vylúčených činností bol teda teleologický alebo účelový, pričom sa nerozlišovali osoby, ktoré ich vykonávali.

71. Z toho teda vyplýva, že vo veci Parlament/Rada a Komisia Súdny dvor vychádzal v prvom rade z cieľa spracovávania údajov. Nezáležalo na tom, že „údaje… zhromaždili súkromní podnikatelia na komerčné účely a že títo podnikatelia zabezpečujú ich prenos do tretej krajiny", lebo rozhodujúce bolo, že „tento prenos… patrí do rámca vytvoreného orgánmi verejnej moci na účely verejnej bezpečnosti".[37]

72. Naopak „činnosti týkajúce sa bezpečnosti štátu", ktoré nepatria do pôsobnosti smernice 2002/58 skúmanej vo veci Tele2 Sverige a Watson, nemôže vykonávať ktorýkoľvek subjekt, ale len samotný štát. Okrem toho ich súčasťou nie sú normatívne alebo regulačné úlohy štátu, ale jedine materiálne činnosti orgánov verejnej moci.

73. *Činnosti* vymenované v článku 1 ods. 3 smernice 2002/58 totiž „sú v každom prípade činnosti patriace štátu alebo štátnym orgánom a nepatria do oblasti činností jednotlivcov".[38] Tieto „činnosti" však nemôžu mať normatívnu povahu. Ak by to tak bolo, všetky ustanovenia prijaté členskými štátmi v súvislosti so spracovávaním osobných údajov by boli vyňaté z pôsobnosti smernice 2002/58, pokiaľ by sa na ich odôvodnenie uviedlo, že sú nevyhnutné na zaručenie bezpečnosti štátu.

74. Na jednej strane by to znamenalo podstatný pokles účinnosti uvedenej smernice, lebo samotné uvedenie takého neurčitého právneho pojmu, akým je pojem národná bezpečnosť, by stačilo na to, aby sa na členské štáty nevzťahovali záruky vytvorené normotvorcom Únie s cieľom chrániť osobné údaje občanov. Túto ochranu nemožno prakticky dosiahnuť bez súčinnosti členských štátov a jej zabezpečenie je pre občana zaručené aj voči vnútroštátnym orgánom verejnej moci.

75. Na druhej strane výklad pojmu „štátne činnosti", ktorý by zahŕňal činnosti, ktoré vedú k prijatiu právnych predpisov a ustanovení, by zbavil zmyslu článok 15 smernice 2002/58, ktorý práve splnomocňuje členské štáty, aby – okrem iného z dôvodov ochrany národnej bezpečnosti – prijali „legislatívne opatrenia" s cieľom obmedziť dosah niektorých práv a povinností stanovených v tejto smernici.[39]

76. Ako Súdny dvor zdôraznil vo veci Tele2 Sverige a Watson, „rozsah pôsobnosti smernice 2002/58 treba posúdiť so zreteľom najmä na všeobecnú systematiku tejto smernice".[40] Z tohto hľadiska je výkladom článku 1 ods. 3 a článku 15 ods. 1 smernice 2002/58, ktorý zaručuje ich zmysel bez straty účinnosti, výklad, podľa ktorého prvé z týchto dvoch ustanovení obsahuje hmotnoprávne vylúčenie týkajúce sa *činností* vykonávaných členskými štátmi v oblasti národnej bezpečnosti (a podobných

37 Rozsudok Parlament/Rada a Komisia, bod 58.

38 Rozsudok Ministerio Fiscal, bod 32. V tom istom zmysle rozsudok Tele2 Sverige a Watson, bod 72.

39 Bolo by totiž ťažké tvrdiť, že článok 15 ods. 1 smernice 2002/58 dovoľuje obmedziť stanovené práva a povinnosti, ktoré proklamuje, v oblasti, ktorá by – tak ako oblasť národnej bezpečnosti – na základe článku 1 ods. 3 tejto smernice bola principiálne vylúčená z jej pôsobnosti. Ako Súdny dvor konštatoval v bode 73 rozsudku Tele2 Sverige a Watson, článok 15 ods. 1 smernice 2002/58 „nevyhnutne predpokladá, že vnútroštátne opatrenia, ktoré sú v ňom uvedené…, spadajú do rozsahu pôsobnosti tejto smernice, pretože táto smernica výslovne dovoľuje členským štátom prijať také opatrenia len za určitých podmienok, ktoré sú v nej stanovené".

40 Rozsudok Tele2 Sverige a Watson, bod 67.

činností) a druhé z týchto dvoch ustanovení obsahuje splnomocnenie na prijatie *legislatívnych opatrení* (teda všeobecne záväzných predpisov), ktoré sa v záujme národnej bezpečnosti dotýkajú činností jednotlivcov podliehajúcich právomoci členských štátov a obmedzujú práva zaručené smernicou 2002/58.

4. Vylúčenie národnej bezpečnosti v smernici 2002/58

77. Národná bezpečnosť (alebo jej synonymum „bezpečnosť štátu“, ako je to zdôraznené v článku 15 ods. 1 tejto smernice) je v smernici 2002/58 zohľadnená dvojako. Na jednej strane predstavuje dôvod *vylúčenia* (uplatnenia tejto smernice) pre všetky tie činnosti členských štátov, ktoré sa jej osobitne „týkajú“. Na druhej strane predstavuje dôvod *obmedzenia* práv a povinností stanovených v smernici 2002/58, ktorý musí byť vymedzený zákonom, teda v súvislosti s činnosťami súkromného alebo obchodného charakteru, ktoré nesúvisia so zvrchovanými činnosťami. [41]

78. Na aké činnosti sa vzťahuje článok 1 ods. 3 smernice 2002/58? Podľa môjho názoru samotná Conseil d'État (Štátna rada) poskytuje dobrý príklad tým, že uvádza články L. 851-5 a L. 851-6 Zákonníka vnútornej bezpečnosti, pričom odkazuje na „metódy zberu informácií, ktoré uplatňuje priamo štát, ale ktoré neupravujú činnosti poskytovateľov elektronických komunikačných služieb tým, že im ukladajú osobitné povinnosti“. [42]

79. Domnievam sa, že práve to je kľúčom na určenie rozsahu vylúčenia uvedeného v článku 1 ods. 3 smernice 2002/58. Jej režimu nepodliehajú *činnosti* zamerané na zachovanie národnej bezpečnosti, ktoré v jej mene vykonávajú orgány verejnej moci bez toho, aby sa vyžadovala spolupráca jednotlivcov, a teda bez toho, aby sa im uložili povinnosti v rámci ich podnikového riadenia.

80. Zoznam činností orgánov verejnej moci, na ktoré sa nevzťahuje všeobecná úprava spracovávania osobných údajov, sa však musí vykladať reštriktívne. Pojem *národná bezpečnosť*, za ktorú v zmysle článku 4 ods. 2 ZEÚ nesie zodpovednosť výlučne každý členský štát, konkrétne nemožno rozšíriť na iné, viac alebo menej blízke oblasti verejného života.

81. Keďže v týchto prejudiciálnych otázkach sú dotknutí jednotlivci (teda subjekty, ktoré poskytujú elektronické komunikačné služby užívateľom) a nejde len o zásah štátnych orgánov, nebude potrebné podrobnejšie sa zaoberať vymedzením čŕt národnej bezpečnosti *stricto sensu*.

82. Domnievam sa však, že ako usmernenie môže poslúžiť kritérium stanovené v rámcovom rozhodnutí 2006/960/SVV [43], ktorého článok 2 písm. a) rozlišuje orgány činné v trestnom konaní v širšom zmysle – ktoré zahŕňajú „vnútroštátny policajný, colný alebo iný orgán, ktorý vnútroštátne právo oprávňuje na odhaľovanie, predchádzanie a vyšetrovanie trestných činov alebo trestnej činnosti a vykonávanie právomoci a prijímanie donucovacích opatrení v súvislosti s takýmito činnosťami“ – na jednej strane a „agentúry alebo jednotky, ktoré sa zaoberajú predovšetkým otázkami národnej bezpečnosti“, na druhej strane [44].

41 Ako generálny advokát Saugmandsgaard Øe mimochodom poznamenal v návrhoch, ktoré predniesol vo veci Ministerio Fiscal (C-207/16, EU:C:2018:300), bod 47), „netreba zamieňať na jednej strane osobné údaje spracúvané *priamo* v rámci činností suverénnej povahy, ktoré vykonáva štát v oblasti patriacej do trestného práva, a na druhej strane údaje spracúvané v rámci činností komerčnej povahy, ktoré vykonáva poskytovateľ elektronických komunikačných služieb, ktoré sú *následne* použité príslušnými štátnymi orgánmi“.

42 Body 18 a 21 návrhu na začatie prejudiciálneho konania vo veci C-511/18.

43 Rámcové rozhodnutie Rady z 18. decembra 2006 o zjednodušení výmeny informácií a spravodajských informácií medzi orgánmi členských štátov Európskej únie činnými v trestnom konaní (Ú. v. EÚ L 386, 2006, s. 89).

44 Článok 1 ods. 4 rámcového rozhodnutia Rady 2008/977/SVV z 27. novembra 2008 o ochrane osobných údajov spracúvaných v rámci policajnej a justičnej spolupráce v trestných veciach (Ú. v. EÚ L 350, 2008, s. 60) v tom istom zmysle stanovoval, že „týmto rámcovým rozhodnutím nie sú dotknuté základné záujmy národnej bezpečnosti ani osobitné spravodajské činnosti v oblasti národnej bezpečnosti“.

83. V odôvodnení 11 smernice 2002/58 sa uvádza, že táto smernica sa „podobne ako smernica 95/46… netýka otázok ochrany základných práv a slobôd vzťahujúcich sa k činnostiam, ktoré nie sú upravené právom [Únie]“. Smernica 2002/58 teda „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… bezpečnosti štátu…“.

84. Existuje totiž spojitosť medzi smernicou 95/46 a smernicou 2002/58, pokiaľ ide o právomoci členských štátov v oblasti národnej bezpečnosti. Predmetom žiadnej z týchto dvoch smerníc nie je ochrana základných práv v tejto špecifickej oblasti, v ktorej činnosti členských štátov nie sú „upravené právom [Únie]“.

85. „Rovnováha“ uvedená v spomenutom odôvodnení vyplýva z potreby rešpektovať právomoci členských štátov v oblasti národnej bezpečnosti, keď ich vykonávajú *priamo a vlastnými prostriedkami*. Naopak, pokiaľ sa vyžaduje, aj z tých istých dôvodov národnej bezpečnosti, spolupráca jednotlivcov, ktorým sú uložené určité povinnosti, táto okolnosť znamená vstup do oblasti (ochrana súkromia, ktorú možno vyžadovať od týchto súkromných subjektov) upravenej právom Únie.

86. Tak smernica 95/46, ako aj smernica 2002/58 sa usilujú dosiahnuť túto rovnováhu tým, že umožňujú, aby práva jednotlivcov mohli byť obmedzené na základe legislatívnych opatrení prijatých štátmi podľa článku 13 ods. 1 prvej uvedenej smernice a článku 15 ods. 1 druhej uvedenej smernice. V tomto ohľade nie je medzi nimi nijaký rozdiel.

87. Pokiaľ ide o nariadenie 2016/679, ktorým sa vytvára (nový) všeobecný rámec na ochranu osobných údajov, jeho článok 2 ods. 2 stanovuje, že toto nariadenie sa nevzťahuje na „spracúvanie osobných údajov“ členskými štátmi „pri vykonávaní činností patriacich do rozsahu pôsobnosti kapitoly 2 hlavy V ZEÚ“.

88. Tak ako v smernici 95/46 bolo spracovávanie osobných údajov charakterizované len jeho účelom bez ohľadu na subjekt, ktorý ho vykonával, v nariadení 2016/679 je vylúčené spracúvanie vymedzené tak jeho účelom, ako aj subjektmi, ktoré ho vykonávajú: z pôsobnosti tohto nariadenia je vyňaté spracúvanie osobných údajov členskými štátmi v rámci *činnosti*, ktorá nepatrí do pôsobnosti práva Únie [článok 2 ods. 2 písm. a) a b)], a spracúvanie osobných údajov orgánmi *na účely boja proti trestným činom a ochrany* pred ohrozením verejnej bezpečnosti. [45]

89. Identifikácia týchto činností verejnej moci musí byť nevyhnutne reštriktívna, lebo inak by právne predpisy Únie v oblasti ochrany súkromia boli zbavené potrebného účinku. Nariadenie 2016/679 upravuje v článku 23 – v súlade s článkom 15 ods. 1 smernice 2002/58 – obmedzenie práv a povinností, ktoré stanovuje, *prostredníctvom legislatívnych opatrení*, ak je to nevyhnutné na zaistenie, okrem iných cieľov, národnej bezpečnosti, obrany alebo verejnej bezpečnosti. Ak by ochrana týchto cieľov opäť postačovala na vymedzenie vylúčenia z pôsobnosti nariadenia 2016/679, odvolávanie sa na bezpečnosť štátu ako odôvodnenie obmedzenia práv zaručených týmto nariadením prostredníctvom legislatívnych opatrení by bolo zbytočné.

90. Tak ako je to v prípade smernice 2002/58, nebolo by koherentné, ak by legislatívne opatrenia uvedené v článku 23 nariadenia 2016/679 (ktorý – pripomínam – povoľuje štátne obmedzenia práv občanov na súkromie z dôvodov bezpečnosti štátu) spadali do pôsobnosti tohto nariadenia a zároveň by skutočnosť, že ide o oblasť bezpečnosti štátu, viedla k tomu, že toto nariadenie by bolo automaticky neuplatniteľné, čo by malo za následok nepriznanie nijakého subjektívneho práva.

45 Z pôsobnosti nariadenia 2016/679 je totiž vylúčené spracúvanie údajov členskými štátmi v rámci *činnosti*, ktorá nepatrí do pôsobnosti práva Únie, popri spracúvaní údajov orgánmi *na účely ochrany* verejnej bezpečnosti.

B. Potvrdenie a možnosti rozpracovania judikatúry Tele2 Sverige a Watson

91. V návrhoch prednesených vo veci C-520/18 podrobne rozoberám [46] judikatúru Súdneho dvora v tejto oblasti a na základe tohto rozboru navrhujem potvrdiť ju, pričom zároveň navrhujem určité spôsoby výkladu na spresnenie jej obsahu.

92. Odkazujem na uvedený rozbor, ktorý nepovažujem za nevyhnutné opakovať v týchto návrhoch, a to len z dôvodov hospodárnosti. Úvahy, ktoré uvediem nižšie, týkajúce sa prejudiciálnych otázok, ktoré položila Conseil d'État (Štátna rada), teda treba chápať tak, že vychádzajú z príslušných častí návrhov vo veci C-520/18.

C. Odpoveď na prejudiciálne otázky

1. O povinnosti uchovávať údaje (prvá prejudiciálna otázka vo veciach C-511/18 a C-512/18 a druhá prejudiciálna otázka vo veci C-512/18)

93. Pokiaľ ide o povinnosť uchovávať údaje uloženú poskytovateľom elektronických komunikačných služieb, vnútroštátny súd sa konkrétne pýta, či

– uvedená povinnosť, ktorú možno uložiť na základe článku 15 ods. 1 smernice 2002/58, predstavuje zásah odôvodnený „právom na bezpečnosť", ktoré zaručuje článok 6 Charty, a požiadavkami národnej bezpečnosti (prvá otázka vo veciach C-511/18 a C-512/18, ako aj tretia otázka vo veci C-511/18),

– smernica 2000/31 dovoľuje uchovávanie údajov, ktoré môžu umožniť identifikáciu osôb, ktoré prispeli k vytvoreniu verejne dostupných obsahov online (druhá otázka vo veci C-512/18).

a) Úvodná úvaha

94. Conseil d'État (Štátna rada) poukazuje na základné práva uznané v článku 7 (rešpektovanie súkromného a rodinného života), článku 8 (ochrana osobných údajov) a článku 11 (sloboda prejavu a právo na informácie) Charty. To sú totiž práva, ktoré podľa Súdneho dvora môžu byť dotknuté povinnosťou uchovávať údaje o prenose dát, ktoré vnútroštátne orgány ukladajú poskytovateľom elektronických komunikačných služieb. [47]

95. Vnútroštátny súd poukazuje aj na právo na bezpečnosť chránené článkom 6 Charty. Uvádza ho skôr ako faktor, ktorý by mohol odôvodniť uloženie uvedenej povinnosti, než ako právo, ktoré by prípadne mohlo byť dotknuté.

96. Súhlasím s Komisiou, že takéto odvolanie sa na článok 6 môže byť nejednoznačné. Tak ako Komisia sa domnievam, že toto ustanovenie sa nemá vykladať v tom zmysle, že môže „ukladať Únii pozitívnu povinnosť prijímať opatrenia zamerané na ochranu osôb pre trestnými činmi". [48]

97. Bezpečnosť zaručená uvedeným článkom Charty nie je totožná s verejnou bezpečnosťou. Inak povedané, s verejnou bezpečnosťou súvisí tak ako ktorékoľvek iné základné právo, keďže verejná bezpečnosť je nevyhnutnou podmienkou výkonu základných práv a slobôd.

46 Body 27 až 68.

47 Pozri v tomto zmysle rozsudok Tele2 Sverige a Watson, bod 92, kde je analogicky citovaný rozsudok Digital Rights, body 25 a 70.

48 Bod 37 písomných pripomienok Komisie.

98. Ako pripomína Komisia, článok 6 Charty zodpovedá článku 5 Európskeho dohovoru o ľudských právach (ďalej len „EDĽP“), ako sa uvádza vo vysvetlivkách k Charte. Zo znenia článku 5 EDĽP vyplýva, že „bezpečnosť“ chránená v tomto článku je výlučne osobná bezpečnosť, chápaná ako záruka práva na osobnú slobodu vo vzťahu k svojvoľnému zatknutiu alebo inému pozbaveniu slobody. V konečnom dôsledku je to istota, že osoba môže byť pozbavená slobody len v prípadoch, za podmienok a v súlade s postupmi, ktoré stanovuje zákon.

99. Ide preto o *osobnú bezpečnosť* týkajúcu sa podmienok, za ktorých možno obmedziť osobnú slobodu osôb [49], a nie o *verejnú bezpečnosť* súvisiacu s existenciou štátu, ktorá je v rozvinutej spoločnosti nevyhnutným predpokladom zosúladenia výkonu verejnej moci s uplatnením práv jednotlivcov.

100. Niektoré vlády však žiadajú, aby sa vo väčšej miere zohľadnilo právo na bezpečnosť v druhom z týchto zmyslov. Súdny dvor ho v skutočnosti neopomenul, ale dokonca ho výslovne spomenul vo svojich rozsudkoch [50] a stanoviskách [51]. Nikdy nepoprel význam cieľov všeobecného záujmu týkajúcich sa ochrany národnej bezpečnosti a verejného poriadku [52], boja proti medzinárodnému terorizmu s cieľom zachovať mier a medzinárodnú bezpečnosť a boja proti závažnej trestnej činnosti na účely zabezpečenia verejnej bezpečnosti [53], ktorý správne označil za „prvoradý“ [54]. Ako Súdny dvor svojho času uviedol, „ochrana verejnej bezpečnosti tiež prispieva k ochrane práv a slobôd iných“. [55]

101. Bolo by možné využiť príležitosť, ktorú poskytujú tieto návrhy na začatie prejudiciálneho konania, na jednoznačnejšie navrhnutie nastolenia rovnováhy medzi právom na bezpečnosť na jednej strane a právom na súkromie a právom na ochranu osobných údajov na druhej strane. Tým by sa zamedzilo námietkam, že právo na súkromie a právo na ochranu osobných údajov sa uprednostňujú na úkor práva na bezpečnosť.

102. Na uvedenú rovnováhu podľa môjho názoru poukazuje odôvodnenie 11 a článok 15 ods. 1 smernice 2002/58, v ktorých sa hovorí o požiadavkách nevyhnutnosti a primeranosti opatrení v *demokratickej spoločnosti*. Pripomínam, že právo na bezpečnosť je nerozlučne späté so samotnou existenciou a zachovaním demokracie, čo odôvodňuje, aby sa toto právo v plnom rozsahu zohľadnilo v rámci hodnotenia uvedenej primeranosti. Inak povedané, hoci je zachovanie zásady dôvernosti údajov v demokratickej spoločnosti prvoradé, nemožno podceniť ani význam bezpečnosti tejto spoločnosti.

103. Kontext, ktorý sa vyznačuje vážnymi a pretrvávajúcimi hrozbami pre národnú bezpečnosť, najmä rizikom terorizmu, teda treba vziať do úvahy v súlade s konštatovaním uvedeným v poslednej vete bodu 119 rozsudku Tele2 Sverige a Watson. Vnútroštátny systém bude môcť primerane reagovať na povahu a intenzitu hrozieb, ktorým čelí, pričom táto reakcia nevyhnutne nemusí byť totožná s reakciou iných členských štátov.

104. Napokon musím dodať, že vyššie uvedené úvahy nebránia tomu, aby v naozaj *výnimočných* situáciách, ktoré sa vyznačujú bezprostrednou hrozbou alebo mimoriadnym nebezpečenstvom, ktoré odôvodňujú oficiálne vyhlásenie krízovej situácie v niektorom členskom štáte, vnútroštátne právne predpisy stanovovali na obmedzený čas možnosť uložiť takú širokú a všeobecnú povinnosť uchovávania údajov, aká sa považuje za nevyhnutnú. [56]

49 Tento výklad podal Európsky súd pre ľudské práva. Pozri najmä rozsudok z 5. júla 2016, Buzadji v. Moldavská republika (ECHR:2016:0705JUD002375507), v § 84 ktorého sa uvádza, že základným účelom práva uznaného v článku 5 EDĽP je zabrániť svojvoľnému alebo neodôvodnenému pozbaveniu osobnej slobody.

50 Rozsudok Digital Rights, bod 42.

51 Stanovisko 1/15 (Dohoda o PNR medzi EÚ a Kanadou) z 26. júla 2017 (ďalej len „stanovisko 1/15“, EU:C:2017:592, bod 149 a citovaná judikatúra).

52 Rozsudok z 15. februára 2016, N. (C-601/15 PPU, EU:C:2016:84, bod 53).

53 Rozsudok Digital Rights, bod 42 a citovaná judikatúra.

54 Tamže, bod 51.

55 Stanovisko 1/15, bod 149.

56 Pozri body 105 až 107 mojich návrhov vo veci C-520/18.

105. V dôsledku toho by sa mala prvá otázka položená v oboch návrhoch na začatie prejudiciálneho konania preformulovať tak, aby bola zameraná skôr na možnosť odôvodniť zásah dôvodmi národnej bezpečnosti. Predmetnom pochybností by teda bola otázka, či je povinnosť uložená prevádzkovateľom elektronických komunikačných služieb zlučiteľná s článkom 15 ods. 1 smernice 2002/58.

b) Posúdenie

1) Kvalifikácia vnútroštátnych predpisov, ako sú opísané v oboch návrhoch na začatie prejudiciálneho konania, z hľadiska judikatúry Súdneho dvora

106. Ak vychádzame z návrhov na začatie prejudiciálneho konania, právna úprava, o ktorú ide v konaniach vo veci samej, ukladá povinnosť ukladať údaje:

– prevádzkovateľom elektronických komunikácií a najmä subjektom, ktoré poskytujú verejnosti prístup ku komunikačným službám online, a

– fyzickým alebo právnickým osobám, ktoré na účely poskytovania verejnosti online, a to aj bezodplatne, zabezpečujú uchovávanie signálov, písaného textu, obrázkov a zvukov alebo správ akéhokoľvek druhu dodaných príjemcami týchto služieb.[57]

107. Prevádzkovatelia musia uchovávať jeden rok od ich zaznamenania informácie, ktoré umožňujú identifikovať užívateľa, údaje o použitých koncových komunikačných zariadeniach, technické vlastnosti, dátum, čas a dĺžku trvania každého hovoru, údaje o vyžiadaných alebo použitých doplnkových službách a ich poskytovateľoch, ako aj údaje, ktoré umožňujú identifikovať jedného alebo viacerých adresátov komunikácie, a v prípade telefonických činností pôvod a polohu komunikácie.[58]

108. Pokiaľ ide osobitne o služby týkajúce sa prístupu na internet a služby týkajúce sa ukladania dát, vnútroštátna právna úprava podľa všetkého vyžaduje uchovávanie IP adries[59], prístupových hesiel, a ak došlo k uzavretiu zmluvy alebo vytvoreniu platobného účtu, druhu uskutočnenej platby, ako aj jej označenia, sumy, dátumu a času transakcie[60].

109. Táto povinnosť uchovávania platí na účely vyšetrovania, odhaľovania a stíhania trestných činov.[61] To znamená, že – ako bude uvedené nižšie – na rozdiel od toho, ako je to v prípade povinnosti *zbierať* údaje o prenose dát a polohe, jediným cieľom povinnosti *uchovávať* tieto údaje nie je predchádzanie terorizmu.[62]

110. Čo sa týka podmienok *prístupu* k uchovávaným údajom, z informácií obsiahnutých v spise vyplýva, že buď sa uplatnia podmienky stanovené pre všeobecný režim (zásah súdneho orgánu), alebo je taký prístup obmedzený na subjekty, ktoré boli jednotlivo určené a splnomocnené so súhlasom premiéra udeleným na základe nezáväzného stanoviska nezávislého správneho orgánu.[63]

57 Vyplýva to z článku L. 851-1 Zákonníka vnútornej bezpečnosti, ktorý odkazuje na článok L. 34-1 Zákonníka pôšt a elektronických komunikácií a na článok 6 zákona č. 2004-575 o dôvere v digitálne hospodárstvo.

58 Je to uvedené v článku R. 10-13 Zákonníka pôšt a elektronických komunikácií.

59 Túto otázku, v súvislosti s ktorou boli na pojednávaní vyjadrené odlišné názory, musí overiť vnútroštátny súd.

60 Článok 1 dekrétu č. 2011-219.

61 Článok R. 10-13 Zákonníka pôšt a elektronických komunikácií.

62 Tak La Quadrature du Net, ako aj Fédération des founisseurs d'accès à Internet associatifs zdôrazňujú široký rozsah cieľov uchovávania, diskrečnú právomoc, ktorú majú orgány, neexistenciu objektívnych kritérií pri ich vymedzení a význam pripisovaný formám trestnej činnosti, ktoré nemožno označiť za závažné.

63 Commission nationale de contrôle des techniques de renseignement (Národná komisia pre kontrolu spravodajských metód). Pozri v tejto súvislosti body 145 až 148 písomných pripomienok francúzskej vlády.

111. Na prvý pohľad je jasné – ako uviedla Komisia [64] –, že údaje, ktoré sa podľa vnútroštátnych predpisov majú uchovávať, sa v podstate zhodujú s údajmi, ktoré Súdny dvor skúmal v rozsudku Digital Rights a v rozsudku Tele2 Sverige a Watson [65]. Tak ako v uvedených veciach, na tieto údaje sa vzťahuje „povinnosť všeobecného a nediferencovaného uchovávania“, ako to Conseil d'État (Štátna rada) úplne otvorene zdôrazňuje na začiatku svojich prejudiciálnych otázok.

112. Ak je to tak – čo v konečnom dôsledku musí posúdiť vnútroštátny súd –, možno len konštatovať, že predmetná právna úprava predstavuje „zásah… do základných práv zakotvených v článkoch 7 a 8 Charty[, ktorý] sa javí ako rozsiahly a treba ho považovať za zvlášť závažný“. [66]

113. Ani jeden z účastníkov konania nespochybnil skutočnosť, že právna úprava, ktorá má tieto znaky, spôsobuje zásah do uvedených práv. Teraz sa touto otázkou netreba podrobnejšie zaoberať, a to ani s cieľom pripomenúť, že porušenie uvedených práv nevyhnutne narúša samotné základy spoločnosti, ktorá chce rešpektovať okrem iných hodnôt aj osobné súkromie chránené Chartou.

114. Z uplatnenia judikatúry vytvorenej v rozsudku Tele2 Sverige a Watson a potvrdenej v rozsudku Ministerio Fiscal by prirodzene vyplynulo tvrdenie, že právna úprava, o akú ide v prejednávanej veci, „ide nad rámec toho, čo je prísne nevyhnutné, a nemožno ju teda považovať za odôvodnenú v demokratickej spoločnosti, ako to vyžaduje článok 15 ods. 1 smernice 2002/58 v spojení s článkami 7, 8 a 11, ako aj článkom 52 ods. 1 Charty“. [67]

115. Právna úprava, o ktorú ide v prejednávanej veci, totiž – tak ako právna úprava skúmaná v rozsudku Tele2 Sverige a Watson – tiež „všeobecne zahŕňa všetkých účastníkov a registrovaných užívateľov a všetky spôsoby elektronickej komunikácie, ako aj všetky údaje o prenose dát [a] nestanovuje žiadne rozlíšenie, obmedzenie alebo výnimku na základe sledovaného cieľa“. [68] V dôsledku toho sa „uplatňuje… aj na osoby, pri ktorých nie je dôvod domnievať sa, že by ich konanie mohlo mať aspoň nepriamu alebo vzdialenú súvislosť so závažnými trestnými činmi“, pričom nepripúšťa žiadnu výnimku, „takže sa uplatňuje aj na osoby, ktorých komunikácia podľa pravidiel vnútroštátneho práva podlieha služobnému tajomstvu“. [69]

116. Sporná právna úprava rovnako „nevyžaduje nijakú súvislosť medzi údajmi, ktorých uchovávanie stanovuje, a hrozbou pre verejnú bezpečnosť. Predovšetkým nie je obmedzená na uchovávanie, ktoré by sa vzťahovalo na údaje z určitého časového obdobia a/alebo z určitej zemepisnej oblasti a/alebo na okruh osôb, ktorý by akýmkoľvek spôsobom bolo možné spájať so závažnými trestnými činmi, ani na osoby, ktorých uchovávané údaje by z iných dôvodov mohli prispieť k boju proti trestnej činnosti“. [70]

117. Z vyššie uvedeného vyplýva, že táto právna úprava „ide nad rámec toho, čo je prísne nevyhnutné, a nemožno ju teda považovať za odôvodnenú v demokratickej spoločnosti, ako to vyžaduje článok 15 ods. 1 smernice 2002/58 v spojení s článkami 7, 8 a 11, ako aj článkom 52 ods. 1 Charty“. [71]

64 Bod 60 písomných pripomienok Komisie.

65 V skutočnosti je okruh týchto údajov trochu širší, lebo v prípade služieb týkajúcich sa prístupu na internet je podľa všetkého tiež stanovené, že treba uchovávať IP adresu alebo prístupové heslá.

66 Rozsudok Tele2 Sverige a Watson, bod 100.

67 Tamže, bod 107.

68 Tamže, bod 105.

69 Tamže.

70 Rozsudok Tele2 Sverige a Watson, bod 106.

71 Tamže, bod 107.

118. Uvedené konštatovania postačovali na to, aby Súdny dvor dospel k záveru, že príslušné vnútroštátne predpisy neboli zlučiteľné s článkom 15 ods. 1 smernice 2002/58, v rozsahu, v akom „na účely boja proti trestnej činnosti stanov[ovali] všeobecné a nediferencované uchovávanie všetkých údajov o prenose dát a polohe všetkých účastníkov a registrovaných užívateľov, týkajúce sa všetkých prostriedkov elektronickej komunikácie“.[72]

119. V tomto prípade vzniká otázka, či judikatúru Súdneho dvora týkajúcu sa uchovávania osobných údajov možno ak nie prehodnotiť, tak aspoň upraviť, pokiaľ je cieľom tohto „všeobecného a nediferencovaného“ uchovávania boj proti terorizmu. Prvá otázka vo veci C-511/18 sa kladie práve „v kontexte, ktorý sa vyznačuje vážnymi a pretrvávajúcimi hrozbami pre národnú bezpečnosť, najmä rizikom terorizmu“.

120. Aj keď je *faktický kontext* uloženia povinnosti uchovávať údaje taký, je nesporné, že jeho *normatívny kontext* nevychádza len z terorizmu. Pravidlá uchovávania údajov a prístupu k nim, o ktorých sa diskutuje v konaní na Conseil d'État (Štátna rada), podmieňujú uvedenú povinnosť cieľmi vyšetrovania, odhaľovania a stíhania trestných činov vo všeobecnosti.

121. V každom prípade by som chcel pripomenúť, že úvahy uvedené v rozsudku Tele2 Sverige a Watson sa týkali aj boja proti terorizmu, no Súdny dvor vtedy nepovažoval za potrebné, aby tento druh trestnej činnosti viedol k zmene jeho judikatúry.[73]

122. Preto sa v zásade domnievam, že na otázku vnútroštátneho súdu, ktorá je zameraná na špecifický charakter teroristickej hrozby, treba odpovedať v rovnakom zmysle, v akom Súdny dvor rozhodol v rozsudku Tele2 Sverige a Watson.

123. Ako som uviedol v návrhoch, ktoré som predniesol vo veci Stichting Brein, „ak nutnosť presného uplatňovania práva nezaväzuje súdy k tomu, aby striktne vychádzali zo zásady *stare decisis*, určite od nich aspoň vyžaduje, aby sa náležite riadili svojím vlastným riešením určitého právneho problému“.[74]

2) Obmedzené uchovávanie údajov so zreteľom na hrozby pre bezpečnosť štátu, vrátane teroristickej hrozby

124. Bolo by napriek tomu možné upraviť alebo doplniť uvedenú judikatúru vzhľadom na jej dôsledky pre boj proti terorizmu alebo pre ochranu štátu pred inými podobnými hrozbami pre národnú bezpečnosť?

125. Už som zdôraznil, že samotné uchovávanie osobných údajov znamená zásah do práv zaručených článkami 7, 8 a 11 Charty.[75] Odhliadnuc od toho, že jeho cieľom je v konečnom dôsledku umožniť v určitom okamihu spätný alebo súbežný *prístup* k údajom[76], samotné uchovávanie údajov, ktoré idú nad rámec toho, čo je prísne nevyhnutné na prenos správy alebo na fakturáciu služieb poskytovaných poskytovateľom, predstavuje nedodržanie obmedzení stanovených v článkoch 5 a 6 smernice 2002/58.

72 Tamže, bod 112.

73 Tamže, bod 103.

74 Vec C-527/15, EU:C:2016:938, bod 41.

75 Ako Súdny dvor pripomenul v bode 124 stanoviska 1/15, „poskytnutie osobných údajov takej tretej osobe, akou je orgán verejnej moci, predstavuje zásah do základného práva zakotveného v článku 7 Charty bez ohľadu na účel neskoršieho využitia poskytnutých informácií. To isté platí v prípade uchovávania osobných údajov, ako aj prístupu k uvedeným údajom na účely ich využitia orgánmi verejnej moci. V tejto súvislosti je irelevantné, či dotknuté informácie týkajúce sa súkromného života majú alebo nemajú citlivú povahu alebo či pre dotknuté osoby z dôvodu tohto zásahu vyplynuli alebo nevyplynuli prípadné nepriaznivé následky“.

76 Ako generálny advokát Cruz Villalón uviedol v bode 72 návrhov, ktoré predniesol vo veci Digital Rights (C-293/12 a C-594/12, EU:C:2013:845), „zhromažďovanie a najmä uchovávanie množstva údajov vytváraných alebo spracúvaných v rámci väčšiny bežných elektronických komunikácií občanov Únie v obrovských databázach predstavuje závažný zásah do ich súkromného života, aj keby iba vytváralo podmienky pre možnosť spätnej kontroly ich osobných, ako aj pracovných aktivít. Zhromažďovanie týchto údajov vytvára podmienky pre sledovanie, ktoré napriek tomu, že sa vykonáva iba spätne pri ich použití, nepretržite, počas celej doby uchovávania údajov, ohrozuje právo občanov Únie na dôvernosť ich súkromného života. Vzniknutý nedefinovateľný pocit sledovania nastoľuje zvlášť naliehavo otázku doby uchovávania údajov“.

126. Užívatelia uvedených služieb (v skutočnosti takmer všetci občania v najrozvinutejších spoločnostiach) majú alebo musia mať legitímne očakávanie, že bez ich súhlasu sa nebudú uchovávať iné ich údaje než tie, ktoré sa uchovávajú v súlade s uvedenými ustanoveniami. Výnimky stanovené v článku 15 ods. 1 smernice 2002/58 treba chápať na základe tohto predpokladu.

127. Ako som už vysvetlil, Súdny dvor v rozsudku Tele2 Sverige a Watson odmietol všeobecné a nediferencované uchovávanie osobných údajov aj v súvislosti s bojom proti terorizmu.[77]

128. Pokiaľ ide o vznesené námietky, judikatúra stanovená v uvedenom rozsudku podľa môjho názoru nepodceňuje teroristickú hrozbu ako mimoriadne závažnú formu trestnej činnosti, ktorej súčasťou je výslovný zámer napadnúť autoritu štátu a destabilizovať alebo zničiť jeho inštitúcie. Boj proti terorizmu je doslova životne dôležitý pre štát a jeho úspešné fungovanie, čo je cieľ všeobecného záujmu, ktorého sa právny štát nemôže vzdať.

129. Prakticky všetky vlády, ktoré sa zúčastnili na konaní, ako aj Komisia zhodne uviedli, že – odhliadnuc od technických ťažkostí, ktoré sú s ním spojené – čiastočné a diferencované uchovávanie osobných údajov by odňalo vnútroštátnym spravodajským službám možnosť získať prístup k informáciám, ktoré sú nevyhnutné na identifikáciu hrozieb pre verejnú bezpečnosť a obranu štátu, ako aj na stíhanie páchateľov teroristických útokov.[78]

130. V súvislosti s týmto názorom považujem za relevantné uviesť, že boj proti terorizmu nemožno posudzovať len z hľadiska jeho účinnosti. Preto je zložitý, ale aj vznešený, ak jeho prostriedky a metódy zodpovedajú požiadavkám právneho štátu, ktorými je predovšetkým podriadenie moci a sily právnym obmedzeniam a najmä právnemu poriadku, ktorého dôvodom a účelom existencie je ochrana základných práv.

131. Kým v prípade terorizmu odôvodnenie jeho prostriedkov nevychádza z iného kritéria, než je kritérium samotnej (a najvyššej) účinnosti jeho útokov na ustanovený poriadok, v prípade právneho štátu sa účinnosť meria spôsobom, ktorý nedovoľuje, aby sa v záujme jeho ochrany upustilo od postupov a záruk, vďaka ktorým sa označuje ako legitímny poriadok. Ak by sa právny štát riadil len samotnou účinnosťou, stratil by črtu, ktorá je preň charakteristická, a v krajných prípadoch by sa sám mohol stať hrozbou pre občana. Nedalo by sa nijako zaručiť, že ak by verejná moc mala k dispozícii príliš rozsiahle nástroje na stíhanie trestných činov, pomocou ktorých by mohla ignorovať alebo porušovať základné práva, jej nekontrolované a úplne neobmedzená činnosť by napokon neohrozila slobodu všetkých.

132. Pripomínam, že efektívnosť verejnej moci je obmedzená neprekonateľnou bariérou, ktorú tvoria základné práva občanov, ktorých obmedzenia môžu byť v súlade s článkom 52 ods. 1 Charty ustanovené len zákonom, pričom musia rešpektovať ich podstatu, „ak je to nevyhnutné a skutočne to zodpovedá cieľom všeobecného záujmu, ktoré sú uznané Úniou, alebo ak je to potrebné na ochranu práv a slobôd iných“.[79]

77 Rozsudok Tele2 Sverige a Watson, bod 103: „nemôže … odôvodniť to, aby sa vnútroštátna právna úprava, ktorá stanovuje všeobecné a nediferencované uchovávanie všetkých údajov o prenose dát a polohe, považovala za nevyhnutnú na účely uvedeného boja“.

78 To tvrdí napríklad francúzska vláda, ktorá na ilustráciu tohto tvrdenia uvádza konkrétne príklady užitočnosti všeobecného uchovávania údajov, ktoré umožnilo štátu reagovať na vážne teroristické útoky, ku ktorým došlo v jej krajine v posledných rokoch (body 107 a 122 až 126 písomných pripomienok francúzskej vlády).

79 Rozsudok z 15. februára 2016, N. (C-601/15 PPU, EU:C:2016:84, bod 50). Ide teda o zložitú rovnováhu medzi verejným poriadkom a slobodou, ktorú som už spomenul a o ktorú sa v zásade usiluje celá právna úprava Únie. Ako príklad možno uviesť smernicu Európskeho parlamentu a Rady (EÚ) 2017/541 z 15. marca 2017 o boji proti terorizmu, ktorou sa nahrádza rámcové rozhodnutie Rady 2002/475/SVV a mení rozhodnutie Rady 2005/671/SVV (Ú. v. EÚ L 88, 2017, s. 6). Zatiaľ čo v článku 20 ods. 1 tejto smernice je stanovené, že členské štáty musia zabezpečiť, aby subjekty, ktoré sú zodpovedné za vyšetrovanie alebo stíhanie teroristických trestných činov, „mali k dispozícii účinné nástroje vyšetrovania“, v jej odôvodnení 21 sa uvádza, že využívanie týchto účinných nástrojov by „malo byť cielené a mali by sa pri ňom zohľadňovať zásada proporcionality a povaha a závažnosť vyšetrovaného trestného činu, a malo by dodržiavať právo na ochranu osobných údajov“.

133. Pokiaľ ide o podmienky, za ktorých by v súlade s rozsudkom Tele2 Sverige a Watson bolo prípustné *cielené* uchovávanie údajov, odkazujem na svoje návrhy vo veci C-520/18. [80]

134. Okolnosti, za ktorých informácie, ktoré majú k dispozícii bezpečnostné služby, umožňujú podporiť dôvodné podozrenie z prípravy teroristického útoku, môžu predstavovať legitímny prípad uloženia povinnosti uchovávať určité údaje. Tým skôr ním môže byť skutočné spáchanie útoku. Kým v tomto poslednom uvedenom prípade spáchanie trestného činu môže byť samo osebe faktorom, ktorý odôvodňuje prijatie uvedeného opatrenia, pokiaľ existuje len podozrenie z prípadného útoku, je potrebné, aby okolnosti, ktoré odôvodňujú jeho prijatie, vykazovali aspoň určitú mieru pravdepodobnosti, ktorá je nevyhnutná pre objektívne zváženie dôkazov, ktoré môžu odôvodniť prijatie tohto opatrenia.

135. Je síce ťažké, no nie nemožné presne a na základe objektívnych kritérií určiť tak kategórie údajov, ktorých uchovávanie sa považuje za nevyhnutné, ako aj okruh dotknutých osôb. *Najpraktickejšie* a *najúčinnejšie* by bolo určite všeobecné a nediferencované uchovávanie všetkých údajov, ktoré môžu zhromažďovať poskytovatelia elektronických komunikačných služieb, ale už som uviedol, že túto otázku nemožno vyriešiť v zmysle *praktickej účinnosti*, ale v zmysle *právnej účinnosti* a v kontexte právneho štátu.

136. Toto vymedzenie je typicky legislatívne, a to v medziach stanovených judikatúrou Súdneho dvora. Opäť odkazujem na úvahy, ktoré v tejto súvislosti uvádzam vo svojich návrhoch vo veci C-520/18. [81]

3) Prístup k uchovávaným údajom

137. Vychádzajúc z predpokladu, že prevádzkovatelia vykonali zber údajov spôsobom, ktorý je v súlade s ustanoveniami smernice 2002/58, a že ich uchovávanie sa uskutočnilo podľa článku 15 ods. 1 [82], prístup príslušných orgánov k týmto informáciám sa musí uskutočniť za podmienok stanovených Súdnym dvorom, ktoré analyzujem v návrhoch prednesených vo veci C-520/18, na ktoré odkazujem [83].

138. Aj v prejednávanej veci musí preto vnútroštátna právna úprava upravovať hmotnoprávne a procesnoprávne podmienky prístupu príslušných orgánov k uchovávaným údajom. [84] V rámci týchto návrhov na začatie prejudiciálneho konania by tieto podmienky umožnili prístup k údajom o osobách, ktoré sú podozrivé z toho, že plánujú spáchať alebo spáchali teroristický čin, alebo môžu byť zapojené do teroristického činu. [85]

139. Podstatné je však to, aby – s výnimkou riadne odôvodnených naliehavých prípadov – prístup k sporným údajom podliehal predbežnému preskúmaniu zo strany súdu alebo nezávislého správneho orgánu, ktorého rozhodnutie je reakciou na odôvodnenú žiadosť príslušných orgánov. [86] Ak sa teda nemôže uplatniť abstraktné posúdenie stanovené zákonom, je zaručené posúdenie *in concreto* týmto nezávislým orgánom, ktorý je rovnako povinný zaručiť bezpečnosť štátu a ochranu základných práv občanov.

80 Body 87 až 95.

81 Body 100 až 107.

82 Za predpokladu, že budú dodržané podmienky uvedené v bode 122 rozsudku Tele2 Sverige a Watson – Súdny dvor pripomenul, že článok 15 ods. 1 smernice 2002/58 nedovoľuje odchýliť sa od článku 4 ods. 1, ani od článku 4 ods. 1a tejto smernice, ktoré vyžadujú, aby poskytovatelia prijali opatrenia na zabezpečenie ochrany uchovávaných údajov pred rizikom zneužitia, ako aj pred nezákonným prístupom. V tomto zmysle konštatoval, že „vzhľadom na množstvo uchovávaných údajov, citlivú povahu týchto údajov, ako aj riziko nezákonného prístupu k nim musia poskytovatelia elektronických komunikačných služieb na účely zaistenia úplnej integrity a dôvernosti týchto údajov zaručovať veľmi vysokú úroveň ochrany a bezpečnosti prostredníctvom primeraných technických a organizačných opatrení. Vnútroštátna právna úprava musí konkrétne stanovovať uchovávanie údajov na území Únie, ako aj nenávratné zničenie údajov po skončení doby ich uchovávania“.

83 Body 52 až 60.

84 Rozsudok Tele2 Sverige a Watson, bod 118.

85 Tamže, bod 119.

86 Tamže, bod 120.

4) Povinnosť uchovávať údaje, ktoré umožňujú identifikovať tvorcov obsahov, z hľadiska smernice 2000/31 (druhá prejudiciálna otázka vo veci C-512/18)

140. Vnútroštátny súd poukazuje na smernicu 2000/31 ako referenčné kritérium na určenie, či možno určitým osobám [87] a prevádzkovateľom, ktorí ponúkajú verejnosti komunikačné služby, uložiť povinnosť uchovávať údaje „umožňujúce zistiť, kto prispel k tvorbe obsahu alebo jedného z obsahov služieb, ktorých sú poskytovateľmi, aby súdny orgán mohol prípadne požiadať o ich poskytnutie na účely uplatňovania predpisov týkajúcich sa občianskoprávnej alebo trestnej zodpovednosti“.

141. Súhlasím s Komisiou, že by nebolo namieste skúmať zlučiteľnosť uvedenej povinnosti so smernicou 2000/31 [88], keďže podľa článku 1 ods. 5 písm. b) tejto smernice sú z jej pôsobnosti vylúčené „otázky týkajúce sa služieb informačnej spoločnosti, na ktoré sa vzťahujú smernice 95/46/ES a 97/66/ES“, pričom týmto predpisom v súčasnosti zodpovedá nariadenie 2006/679 a smernica 2002/58 [89], ktorých článok 23 ods. 1, resp. článok 15 ods. 1 sa podľa môjho názoru majú vykladať vo vyššie uvedenom zmysle.

2. O povinnosti zbierať v reálnom čase údaje o prenose dát a polohe (druhá prejudiciálna otázka vo veci C-511/18)

142. Podľa vnútroštátneho súdu článok L. 851-2 Zákonníka vnútornej bezpečnosti povoľuje – iba na účely predchádzania terorizmu – zbierať v reálnom čase informácie o osobách vopred označených ako osoby, v prípade ktorých existuje podozrenie, že majú väzbu s teroristickou hrozbou. Článok L. 851-4 tohto zákonníka rovnako dovoľuje, aby prevádzkovatelia v reálnom čase prenášali technické údaje týkajúce sa polohy koncových zariadení.

143. Podľa vnútroštátneho súdu tieto metódy neukladajú poskytovateľom požiadavku dodatočného uchovávania v porovnaní s tým, čo je potrebné na fakturáciu ich služieb a uvádzanie týchto služieb na trh.

144. Okrem toho v zmysle článku L. 851-3 Zákonníka vnútornej bezpečnosti možno prevádzkovateľom elektronických komunikácií a poskytovateľom technických služieb uložiť povinnosť týkajúcu sa „uplatňovania automatizovaných procesov spracovávania v ich sieťach na zisťovanie pripojení, ktoré by mohli predstavovať teroristickú hrozbu, v závislosti od parametrov určených v povolení“. Táto metóda nemá za následok všeobecné a nediferencované uchovávanie údajov a jej cieľom je vyzbierať počas obmedzenej doby tie údaje o pripojení, ktoré by mohli súvisieť s teroristickým trestným činom.

145. Podľa môjho názoru sa podmienky, ktoré musí spĺňať prístup k uchovávaným osobným údajom, musia vzťahovať aj na prístup k údajom vytvoreným v priebehu elektronickej komunikácie poskytovaný v reálnom čase. Odkazujem teda na to, čo som uviedol v súvislosti s touto problematikou. Nie je rozhodujúce, či ide o uchovávané údaje alebo okamžite získané údaje, lebo v oboch prípadoch dochádza k poskytnutiu osobných údajov, pričom nezáleží na tom, či ide o minulé alebo súčasné údaje.

87 Ide o osoby, ktoré „na účely poskytovania verejnosti prostredníctvom verejných komunikačných služieb online… zabezpečujú uchovávanie signálov, písaného textu, obrázkov a zvukov alebo správ akéhokoľvek druhu dodaných príjemcami týchto služieb…“.

88 Vnútroštátny súd všeobecne spomína túto smernicu v druhej otázke vo veci C-512/18, pričom neuvádza nijaké konkrétne ustanovenie.

89 Body 112 a 113 písomných pripomienok Komisie.

146. Ak by prístup v reálnom čase vyplýval z pripojení zistených pomocou automatizovaného spracovávania, aké je uvedené v článku L. 851-3 Zákonníka vnútornej bezpečnosti, konkrétne sa vyžaduje, aby vzory a kritériá vopred stanovené pre toto spracovávanie boli konkrétne, spoľahlivé a nediskriminačné, aby umožnili identifikovať jednotlivcov, vo vzťahu ku ktorým môže existovať dôvodné podozrenie z účasti na teroristických trestných činoch. [90]

3. O povinnosti informovať dotknuté osoby (tretia prejudiciálna otázka vo veci C-511/18)

147. Súdny dvor konštatoval, že orgány, ktorým bol udelený prístup k údajom, musia informovať o tejto skutočnosti dotknuté osoby, pokiaľ to neohrozí prebiehajúce vyšetrovanie. Dôvod uvedenej povinnosti spočíva v tom, že táto informácia je nevyhnutná na to, aby uvedené osoby mohli vykonať svoje právo na opravný prostriedok výslovne stanovený v článku 15 ods. 2 smernice 2002/58 v prípade, že ich práva boli porušené. [91]

148. Conseil d'État (Štátna rada) sa svojou treťou otázkou vo veci C-511/18 pýta, či uvedená požiadavka informovania nevyhnutne platí v každom prípade, alebo či od nej možno upustiť, ak boli stanovené iné záruky, ako sú tie, ktoré tento súd opisuje vo svojom návrhu na začatie prejudiciálneho konania.

149. Podľa opisu, ktorý uvádza vnútroštátny súd [92], spomenuté záruky spočívajú v možnosti osôb, ktoré chcú overiť, či určitá spravodajská metóda nebola uplatnená protiprávne, obrátiť sa na samotnú Conseil d'État (Štátna rada). Tento orgán môže prípadne v rámci konania, ktoré sa neriadi zásadou kontradiktórnosti charakteristickou pre súdne konania, zrušiť povolenie týkajúce sa opatrenia a naradiť zničenie vyzbieraných informácií.

150. Vnútroštátny súd zastáva názor, že uvedená právna úprava neporušuje právo na účinnú súdnu ochranu. Domnievam sa však, že by sa to teoreticky mohlo uznať v prípade osôb, ktoré sa rozhodnú overiť, či sa na vzťahuje spravodajská činnosť. Naopak uvedené právo nie je dodržané, ak osoby, na ktoré sa vzťahuje alebo vzťahovala táto činnosť, nie sú upovedomené o tejto skutočnosti, a preto ani nemôžu overiť, či ich práva boli alebo neboli porušené.

151. Súdne záruky, na ktoré poukazuje vnútroštátny súd, sú podľa všetkého podmienené iniciatívou osoby, ktorá má podozrenie, že sa zbierajú informácie o nej. Všetci však musia mať účinný prístup k súdu na obranu svojich práv, čo znamená, že osoba, ktorej osobné údaje boli spracované, musí mať možnosť napadnúť na súde zákonnosť tohto spracovania, a teda musí byť upovedomená o tomto spracovaní.

152. Ako vyplýva z poskytnutých informácií, súd síce môže začať konanie *ex offo* alebo na základe podnetu správneho orgánu, ale dotknutej osobe treba v každom prípade umožniť, aby sama začala konanie, čo si vyžaduje, aby jej bolo oznámené, že jej osobné údaje boli určitým spôsobom spracované. Obrana jej práv nemôže závisieť od toho, že sa o tomto spracovaní dozvie od tretích osôb alebo vlastnými prostriedkami.

153. Pokiaľ to teda neohrozí priebeh vyšetrovania, pre ktoré bol poskytnutý prístup k uchovávaným údajom, dotknutej osobe sa musí oznámiť, že tieto údaje boli sprístupnené.

90 Rozsudok Digital Rights, bod 59.

91 Rozsudok Tele2 Sverige a Watson, bod 121.

92 Body 8 až 11 návrhu na začatie prejudiciálneho konania.

154. Odlišnou otázkou je, či v prípade ak dotknutá osoba po tom, čo jej bolo oznámené, že došlo k sprístupneniu jej údajov, podá žalobu, nadväzujúce súdne konanie je v súlade s požiadavkami dôvernosti a utajenia súvisiacimi s preskúmaním postupu orgánov verejnej moci v takých citlivých oblastiach, ako je oblasť bezpečnosti a obrany štátu. Uvedená otázka však nesúvisí s týmito návrhmi na začatie prejudiciálneho konania, a preto podľa môjho názoru nie je opodstatnené, aby o nej Súdny dvor rozhodol.

V. Návrh

155. Na základe vyššie uvedeného navrhujem, aby Súdny dvor odpovedal na prejudiciálne otázky, ktoré mu položila Conseil d'État (Štátna rada, Francúzsko), takto:

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

1. bráni vnútroštátnej právnej úprave, ktorá v kontexte, ktorý sa vyznačuje vážnymi a pretrvávajúcimi hrozbami pre národnú bezpečnosť, najmä rizikom terorizmu, ukladá prevádzkovateľom a poskytovateľom elektronických komunikačných služieb povinnosť všeobecne a nediferencovane uchovávať údaje o prenose dát a polohe všetkých účastníkov, ako aj údaje, ktoré umožňujú identifikovať tvorcov obsahov ponúkaných poskytovateľmi uvedených služieb;

2. bráni vnútroštátnej právnej úprave, ktorá nestanovuje povinnosť informovať dotknuté osoby o spracovávaní ich osobných údajov, ktoré vykonávajú príslušné orgány, okrem prípadu, že by toto oznámenie ohrozilo činnosť uvedených orgánov;

3. nebráni vnútroštátnej právnej úprave, ktorá dovoľuje zbierať v reálnom čase údaje o prenose dát a polohe konkrétnych osôb, pokiaľ sa tieto úkony uskutočňujú v súlade s postupmi stanovenými pre prístup k legálne uchovávaným osobným údajom a s rovnakými zárukami.