Zbierka súdnych rozhodnutí

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

Vec C-520/18

Ordre des barreaux francophones et germanophone,
Académie Fiscale ASBL,
UA,
Liga voor Mensenrechten ASBL,
Ligue des Droits de l'Homme ASBL,
VZ,
WY,
XX
proti
Conseil des ministres,
za účasti:
Child Focus

[návrh na začatie prejudiciálneho konania, ktorý podal Cour constitutionnelle (Ústavný súd, Belgicko)

„Návrh na začatie prejudiciálneho konania – Spracovávanie osobných údajov a ochrana súkromia v sektore elektronických komunikácií – Smernica 2002/58/ES – Pôsobnosť – Článok 1 ods. 3 – Článok 15 ods. 1 – Článok 4 ods. 2 ZEÚ – Charta základných práv Európskej únie – Články 4, 6, 7, 8, 11 a článok 52 ods. 1 – Všeobecná a nediferencovaná povinnosť uchovávať údaje o prenose dát a polohe – Efektívnosť vyšetrovania trestných činov a iné ciele verejného záujmu“

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;

[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).

– 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.

2. Uvedené rozsudky (najmä druhý z nich) znepokojujú orgány niektorých členských štátov, ktoré 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 štátov podporujú zrušenie alebo úpravu uvedenej judikatúry.

3. Niektoré 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 sa za týchto okolností uplatnila uvedená smernica, bolo by 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.

5. Cour constitutionnelle (Ústavný súd, Belgicko) po vydaní rozsudku Digital Rights zrušil vnútroštátnu právnu úpravu, ktorou bola do vnútroštátneho práva čiastočne prebratá smernica 2006/24, ktorá bola v uvedenom rozsudku vyhlásená za neplatnú. Belgický zákonodarca potom prijal novú právnu úpravu, ktorej zlučiteľnosť s právom Únie bola opäť spochybnená na základe rozsudku Tele2 Sverige a Watson.

6. Prejednávaný návrh na začatie prejudiciálneho konania je špecifický tým, že poukazuje na možnosť dočasne zachovať účinky vnútroštátneho predpisu, ktorý musia vnútroštátne súdy z dôvodu jeho nezlučiteľnosti s právom Únie vyhlásiť za neplatný.

I. Právny rámec

A. Právo Únie

7. Odkazujem na príslušný bod svojich návrhov vo veciach C-511/18 a C-512/18.

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).

7 Okrem tejto veci (vec C-520/18, Ordre des barreaux francophones et germanophone a i.) ide o veci C-511/18 a C-512/18, La Quadrature du Net a i., a vec C-623/17, Privacy International.

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.

B. Vnútroštátne právo. Loi du 29 mai 2016 relative à la collecte et à la conservation des données dans le secteur des communications électroniques [11]

8. Článok 4 stanovuje, že článok 126 loi du 13 juin 2005 relative aux communications électroniques [12] znie takto:

„(1) Bez toho, aby boli dotknuté ustanovenia zákona z 8. decembra 1992 o ochrane súkromného života s ohľadom na spracovanie osobných údajov [zákon z 8. decembra 1992 o ochrane súkromného života s ohľadom na spracovanie osobných údajov], poskytovatelia verejných telefonických služieb, vrátane telefonických služieb cez internet, pripojenia na internet, elektronickej pošty cez internet, operátori, ktorí prevádzkujú verejné elektronické komunikačné siete, ako aj operátori poskytujúci niektorú z týchto služieb uchovávajú údaje uvedené v odseku 3, ktoré vytvárajú alebo spracúvajú v rámci poskytovania predmetných komunikačných služieb.

Tento článok sa nevzťahuje na obsah komunikácie.

…

(2) Iba nasledujúce orgány sú na základe jednoduchej žiadosti oprávnené získať od poskytovateľov a operátorov uvedených v odseku 1 prvom pododseku údaje uchovávané podľa tohto článku na účely a za podmienok uvedených nižšie:

1. súdne orgány na účely pátrania, vyšetrovania a stíhania trestných činov, na účely vykonania opatrení uvedených v článkoch 46a a 88a zákona o trestnom súdnom konaní (Trestný poriadok) a za podmienok uvedených v týchto článkoch;

2. spravodajské a bezpečnostné služby na plnenie spravodajských úloh pomocou metód zberu údajov uvedených v článkoch 16/2, 18/7 a 18/8 loi du 30 novembre 1998 organique des services de renseignement et de sécurité [13] a za podmienok stanovených týmto zákonom…;

3. každý príslušník justičnej polície Institut belge des services postaux et des télécommunications (Belgický inštitút pre poštové služby a telekomunikácie, ďalej len ‚Inštitút') na účely pátrania, vyšetrovania a stíhania porušení [pravidiel bezpečnosti sietí] a tohto článku;

4. tiesňové služby, ktoré poskytujú pomoc na mieste, ak po uskutočnení tiesňového hovoru nezískajú od príslušného poskytovateľa alebo operátora identifikačné údaje volajúceho… alebo získajú neúplné alebo nesprávne údaje. Možno požadovať výlučne identifikačné údaje volajúceho, a to najneskôr do 24 hodín od uskutočnenia hovoru;

5. príslušník justičnej polície Cellule des personnes disparues de la Police Fédérale (Jednotka nezvestných osôb Federálnej polície) v rámci plnenia svojej úlohy spočívajúcej v poskytnutí pomoci ohrozenej osobe, v pátraní po osobách, ktorých zmiznutie je znepokojujúce, pokiaľ existuje predpoklad alebo dôvodné podozrenie, že je bezprostredne ohrozená telesná integrita nezvestnej osoby. Príslušník policajného útvaru povereného kráľom môže operátora alebo

11 Zákon z 29. mája 2016 o zbere a uchovávaní údajov v odvetví elektronických komunikácií (ďalej len „zákon z 29. mája 2016"; Moniteur belge z 18. júla 2016, s. 44717).

12 Zákon z 13. júna 2005 o elektronických komunikáciách (ďalej len „zákon z roku 2005"; *Moniteur belge* z 20. júna 2005, s. 28070).

13 Organický zákon z 30. novembra 1998 o spravodajských a bezpečnostných službách (ďalej len „zákon z roku 1998"; *Moniteur belge* z 18. decembra 1998, s. 40312).

poskytovateľa žiadať výlučne o poskytnutie údajov o nezvestnej osobe uvedených v odseku 3 prvom a druhom pododseku, ktoré boli uchovávané počas 48 hodín pred predložením žiadosti o poskytnutie údajov;

6. Service de médiation pour les télécommunications (Mediačná služba pre oblasť telekomunikácií) na účely identifikácie osoby, ktorá zneužila sieť alebo službu elektronickej komunikácie… Možno žiadať výlučne o identifikačné údaje.

Poskytovatelia a operátori uvedení v odseku 1 prvom pododseku zabezpečia, aby boli údaje uvedené v odseku 3 dostupné bez obmedzení z územia Belgicka a aby bolo tieto údaje a akékoľvek iné potrebné informácie týkajúce sa týchto údajov možné poskytnúť bezodkladne a výlučne orgánom uvedeným v tomto odseku.

Bez toho, aby tým boli dotknuté iné zákonné ustanovenia, poskytovatelia a operátori uvedení v odseku 1 prvom pododseku nie sú oprávnení použiť údaje uchovávané v zmysle odseku 3 na iné účely.

(3) Údaje umožňujúce identifikáciu používateľa alebo účastníka a komunikačných prostriedkov, okrem údajov osobitne uvedených v odsekoch 2 a 3, sa uchovávajú po dobu dvanástich mesiacov odo dňa, keď sa komunikácia môže s pomocou využívanej služby uskutočniť poslednýkrát.

Údaje o prístupe a pripojení koncového zariadenia k sieti a k službe, ako aj údaje o polohe tohto zariadenia, vrátane koncového bodu siete, sa uchovávajú po dobu dvanástich mesiacov od dátumu komunikácie.

Údaje o komunikácii okrem obsahu, vrátane ich pôvodu a cieľa, sa uchovávajú po dobu dvanástich mesiacov od dátumu komunikácie.

Kráľ nariadením prijatým Conseil des ministres (Rada ministrov) na návrh ministre de la Justice (minister spravodlivosti) a [príslušného] ministra po vyjadrení Commission de la protection de la vie privée (Komisia pre ochranu súkromia) a Inštitútu určí údaje, ktoré sa majú uchovávať v každej z kategórií uvedených v odsekoch 1 a 3, spolu s požiadavkami, ktoré musia tieto údaje spĺňať.

(4) Na účely uchovávania údajov uvedených v odseku 3 poskytovatelia a operátori uvedení v odseku 1 prvom pododseku:

1. zabezpečia, že uchovávané údaje majú rovnakú kvalitu a že sa na ne vzťahujú rovnaké požiadavky bezpečnosti a ochrany ako na údaje nachádzajúce sa v sieti;

2. dohliadajú na to, aby uchovávané údaje boli predmetom vhodných technických a organizačných opatrení s cieľom chrániť ich pred náhodným alebo nezákonným zničením, náhodnou stratou alebo zmenou alebo nepovoleným alebo nezákonným zálohovaním, spracovaním, sprístupnením alebo zverejnením;

3. zabezpečia, že prístup k uchovávaným údajom v rámci odpovede na žiadosti orgánov uvedených v odseku 2 získa len jeden alebo viacerí členovia koordinačnej jednotky uvedenej v článku 126/1 ods. 1;

4. uchovávajú údaje na území Európskej únie;

5. uplatnia opatrenia technickej ochrany, ktoré zabezpečia, že uchovávané údaje sa od okamihu ich zaznamenania stanú nečitateľnými a nepoužiteľnými pre akúkoľvek osobu, ktorá nemá povolený prístup k takýmto údajom;

6. bez toho, aby boli dotknuté články 122 a 123, vymažú uchovávané údaje zo všetkých nosičov po uplynutí doby uchovávania vzťahujúcej sa na tieto údaje stanovenej v odseku 3;

7. zabezpečia možnosť vysledovať spôsob použitia uchovávaných údajov v prípade každej žiadosti orgánu uvedeného v odseku 2 o poskytnutie týchto údajov.

Možnosť vysledovania uvedená v odseku 1 bode 7 sa uskutočňuje pomocou denníka. Inštitút a Komisia pre ochranu súkromia môžu nahliadnuť do tohto denníka a vyžiadať si kópiu celého denníka alebo jeho časti. Inštitút a Komisia pre ochranu súkromia uzavrú protokol o spolupráci týkajúci sa oboznamovania sa s obsahom denníka a jeho kontroly.

(5) Minister a minister spravodlivosti každý rok predloží Poslaneckej snemovni štatistiky o uchovávaní údajov vytvorených alebo spracovaných v rámci poskytovania verejne dostupných komunikačných služieb alebo sietí.

Tieto štatistiky zahŕňajú najmä:

1. prípady, v ktorých boli údaje poskytnuté príslušným orgánom v súlade s uplatniteľnými právnymi predpismi;

2. dobu, ktorá uplynula odo dňa uchovania údajov do dňa, keď príslušné orgány požiadali o ich poskytnutie;

3. prípady, v ktorých nebolo možné vyhovieť žiadostiam o poskytnutie údajov.

Tieto štatistiky nemôžu zahŕňať osobné údaje.

…“

9. Článok 5 stanovuje, že do zákona z roku 2005 sa vkladá článok 126/1 s týmto znením:

„(1) V rámci každého operátora a v rámci každého poskytovateľa uvedeného v článku 126 odseku 1 prvom pododseku sa zriadi koordinačná jednotka poverená poskytovaním údajov uchovávaných v súlade s článkami 122, 123 a 126, identifikačných údajov volajúceho podľa článku 107 ods. 2 prvého pododseku alebo údajov, ktoré možno požadovať na základe článkov 46a, 88a a 90c zákona o trestnom súdnom konaní a článkov 18/7, 18/8, 18/16 a 18/17 [zákona z roku 1998], belgickým orgánom určeným zákonom na základe ich žiadosti.

…

(2) Operátori a poskytovatelia uvedení v článku 126 ods. 1 prvom pododseku stanovia vnútorné postupy umožňujúce odpovedať na žiadosti orgánov o sprístupnenie osobných údajov týkajúcich sa používateľov. Na požiadanie poskytnú Inštitútu informácie o týchto postupoch, o počte prijatých žiadostí, o uplatnenom právnom základe a o odpovedi.

…

(3) Poskytovatelia a operátori uvedení v článku 126 ods. 1 prvom pododseku určia jednu alebo viaceré osoby zodpovedné za ochranu osobných údajov, ktoré musia spĺňať kumulatívne podmienky vymenované v odseku 1 treťom pododseku.

…

Pri výkone svojich úloh koná osoba zodpovedná za ochranu osobných údajov úplne nezávisle a má prístup ku všetkým osobným údajom, ktoré boli poskytnuté orgánom, ako aj do všetkých relevantných priestorov poskytovateľa alebo operátora.

…

(4) Kráľ nariadením prijatým Radou ministrov po vyjadrení Komisie pre ochranu súkromia a Inštitútu určí:

…

2. požiadavky, ktoré musí spĺňať koordinačná jednotka, pričom v tejto súvislosti prihliadne na situáciu operátorov a poskytovateľov, ktorí prijímajú nízky počet žiadostí od justičných orgánov, nemajú sídlo v Belgicku alebo svoju činnosť vykonávajú prevažne zo zahraničia;

3. informácie, ktoré sa majú poskytnúť Inštitútu a Komisii pre ochranu súkromia v súlade s odsekmi 1 a 3, ako aj orgány, ktoré majú prístup k týmto informáciám;

4. ostatné pravidlá, ktorými sa riadi spolupráca operátorov a poskytovateľov uvedených v článku 126 ods. 1 prvom pododseku s belgickými orgánmi alebo niektorými z nich pri poskytovaní údajov uvedených v odseku 1, ak je to potrebné vrátane formy a obsahu žiadosti podľa dotknutého orgánu.

…“

10. Článok 8 stanovuje, že článok 46a ods. 1 Trestného poriadku znie takto:

„(1) Pri vyšetrovaní zločinov a prečinov môže kráľovský prokurátor na základe odôvodneného písomného rozhodnutia – v prípade potreby po požiadaní operátora elektronickej komunikačnej siete alebo poskytovateľa elektronickej komunikačnej služby alebo policajného útvaru určeného kráľom – na základe všetkých údajov, ktoré má k dispozícii, alebo po nahliadnutí do spisov zákazníkov operátorov alebo poskytovateľov služieb pristúpiť alebo nariadiť, aby sa pristúpilo k:

1. identifikácii účastníka alebo obvyklého používateľa elektronickej komunikačnej služby alebo použitého prostriedku elektronickej komunikácie;

2. identifikácii elektronických komunikačných služieb, ktoré si určitá osoba predplatila alebo ktoré určitá osoba obvykle využíva.

Odôvodnenie odráža primeranú povahu s ohľadom na rešpektovanie súkromného života a subsidiárny charakter voči akejkoľvek inej vyšetrovacej povinnosti.

V prípade obzvlášť naliehavej potreby môže každý príslušník justičnej polície s predchádzajúcim ústnym súhlasom kráľovského prokurátora odôvodneným písomným rozhodnutím požiadať

o tieto údaje. Príslušník justičnej polície toto odôvodnené písomné rozhodnutie, ako aj získané informácie poskytne kráľovskému prokurátorovi do 24 hodín a navyše odôvodní obzvlášť naliehavú potrebu.

Ak ide o trestné činy, za ktoré nemožno uložiť hlavný trest odňatia slobody v trvaní jedného roka alebo prísnejší trest, kráľovský prokurátor alebo v prípade obzvlášť naliehavej potreby príslušník justičnej polície môže požiadať o údaje uvedené v odseku 1 len za šesť mesiacov pred vydaním svojho rozhodnutia.

(2) Každý operátor elektronickej komunikačnej siete a každý poskytovateľ elektronických komunikačných služieb, ktorý bol požiadaný, aby oznámil údaje uvedené v odseku 1, poskytne kráľovskému prokurátorovi alebo príslušníkovi justičnej polície údaje, o ktoré bol požiadaný, v lehote, ktorú určí kráľ.…

…

Každý, kto sa z dôvodu svojej funkcie dozvie o opatrení alebo v rámci neho poskytuje súčinnosť, je povinný zachovávať mlčanlivosť. Každé porušenie mlčanlivosti sa potrestá v súlade s článkom 458 Trestného zákona.

Odmietnutie poskytnúť údaje sa trestá pokutou od 26 eur do 10 000 eur.“

11. Článok 9 stanovuje, že článok 88a Trestného poriadku má nasledujúce znenie:

„(1) Ak existujú vážne dôvody, na základe ktorých sa možno domnievať, že za trestné činy možno uložiť hlavný trest odňatia slobody v trvaní jedného roka alebo prísnejší trest, a ak sa sudca pre prípravné konanie domnieva, že existujú okolnosti, ktoré si na účely preukázania pravdy vyžadujú zistenie presnej polohy elektronickej komunikácie alebo lokalizovanie pôvodu alebo cieľa elektronickej komunikácie, môže – v prípade potreby po tom, čo priamo alebo prostredníctvom policajného útvaru určeného kráľom požiada operátora elektronickej komunikačnej siete alebo poskytovateľa elektronickej komunikačnej služby o technickú pomoc – pristúpiť alebo nariadiť, aby sa pristúpilo k:

1. zisteniu presnej polohy údajov o prenose dát na prostriedkoch elektronickej komunikácie, z ktorých alebo do ktorých smeruje alebo smerovala elektronická komunikácia;

2. lokalizácii pôvodu alebo cieľa elektronickej komunikácie.

V prípadoch uvedených odseku 1 sa pre každý prostriedok elektronickej komunikácie, v prípade ktorého sa zaznamenajú údaje o hovore alebo v prípade ktorého sa lokalizuje pôvod alebo cieľ telekomunikácie, uvedie a zaznamená do zápisnice deň, hodina a trvanie a v prípade potreby aj miesto elektronickej komunikácie.

Sudca pre prípravné konanie uvedie v odôvodnenom uznesení skutkové okolnosti veci, ktoré odôvodňujú opatrenie, jeho primeranú povahu s ohľadom na rešpektovanie súkromného života a subsidiárny charakter vo vzťahu k akejkoľvek inej vyšetrovacej povinnosti.

Okrem toho spresní dobu, počas ktorej sa opatrenie môže uplatniť v budúcnosti, pričom táto doba nesmie presiahnuť dva mesiace od okamihu vydania uznesenia, s možnosťou predĺženia, a prípadne obdobie v minulosti, na ktoré sa uznesenie vzťahuje v súlade s odsekom 2.

…

(2) V súvislosti s uplatňovaním opatrenia uvedeného v odseku 1 prvom pododseku na údaje o prenose dát alebo polohe uchovávané na základe článku 126 [zákona z roku 2005] sa použijú tieto ustanovenia:

– v prípade trestného činu uvedeného v knihe II oddiele 1c Trestného zákona môže sudca pre prípravné konanie vo svojom uznesení vyžiadať údaje za obdobie dvanástich mesiacov pred vydaním uznesenia;

– v prípade iného trestného činu uvedeného v článku 90c ods. 2 až 4, ktorý sa neuvádza v prvej zarážke, alebo v prípade trestného činu, ktorý bol spáchaný v rámci zločineckej organizácie uvedenej v článku 324a Trestného zákona, alebo v prípade trestného činu, za ktorý možno uložiť hlavný trest odňatia slobody v trvaní piatich rokov alebo prísnejší trest, môže sudca pre prípravné konanie vo svojom uznesení vyžiadať údaje za obdobie deviatich mesiacov pred vydaním uznesenia;

– v prípade iného trestného činu môže sudca pre prípravné konanie vyžiadať údaje iba za obdobie šiestich mesiacov pred vydaním uznesenia.

(3) Opatrenie sa nesmie týkať prostriedkov elektronickej komunikácie advokáta alebo lekára, ibaže je sám podozrivý zo spáchania trestného činu uvedeného v odseku 1 alebo z účasti na ňom alebo sa na základe konkrétnych skutočností možno domnievať, že tretie osoby podozrivé zo spáchania trestného činu uvedeného v odseku 1 využívajú jeho prostriedky elektronickej komunikácie.

Opatrenie možno vykonať iba po predchádzajúcom upozornení predsedu advokátskej komory alebo prípadne zástupcu miestnej lekárskej komory. Sudca pre prípravné konanie oboznámi tieto osoby so skutočnosťami, ktoré považuje za súčasť profesijného tajomstva. Tieto skutočnosti sa neuvedú do zápisnice. …

(4) Každý, kto sa z dôvodu svojej funkcie dozvie o opatrení alebo v rámci neho poskytuje súčinnosť, je povinný zachovávať mlčanlivosť. Každé porušenie mlčanlivosti sa potrestá v súlade s článkom 458 Trestného zákona.

…“

12. Podľa článku 12 má článok 13 zákona z roku 1998 nasledujúce znenie:

„Spravodajské a bezpečnostné služby môžu vyhľadávať, zbierať, prijímať a spracúvať informácie a osobné údaje, ktoré môžu byť užitočné pre plnenie ich úloh, a aktualizovať dokumentáciu týkajúcu sa predovšetkým udalostí, skupín a osôb, ktoré sú relevantné pre plnenie ich úloh.

Informácie uvedené v dokumentácii musia súvisieť s účelom spisu a obmedziť sa na požiadavky, ktoré z neho vyplývajú.

Spravodajské a bezpečnostné služby dbajú o bezpečnosť údajov týkajúcich sa ich zdrojov a o bezpečnosť informácií a osobných údajov poskytnutých týmito zdrojmi.

Agenti spravodajských a bezpečnostných služieb majú prístup k informáciám, správam a osobným údajom, ktoré zozbierala a spracovala ich služba, v rozsahu, v akom sú tieto informácie užitočné pre výkon ich funkcií alebo plnenie ich úloh.“

13. Článok 14 stanovuje nové znenie článku 18/3, ktorý v súčasnosti znie takto:

„(1) Osobitné metódy získavania údajov uvedené v článku 18/2 ods. 1 možno uplatniť s ohľadom na hroziace nebezpečenstvo uvedené v článku 18/1, ak sa obvyklé metódy získavania údajov považujú za nedostatočné na to, aby umožnili získať informácie potrebné na dokončenie spravodajskej úlohy. Osobitná metóda sa musí zvoliť s ohľadom na stupeň závažnosti hroziaceho nebezpečenstva, pre ktoré sa uplatňuje.

Osobitnú metódu možno uplatniť len na základe odôvodneného písomného rozhodnutia vedúceho útvaru a po oznámení tohto rozhodnutia komisii.

(2) V rozhodnutí vedúceho útvaru sa uvedie:

1. povaha osobitnej metódy;

2. podľa konkrétneho prípadu fyzické alebo právnické osoby, združenia alebo skupiny, veci, miesta, udalosti alebo informácie, na ktoré sa vzťahuje osobitná metóda;

3. hroziace nebezpečenstvo, ktoré odôvodňuje použitie osobitnej metódy;

4. skutkové okolnosti, ktoré odôvodňujú použitie osobitnej metódy, odôvodnenie subsidiarity a primeranosti, vrátane súvislosti medzi bodmi 2 a 3;

5. doba, počas ktorej sa môže osobitná metóda uplatňovať, od okamihu oznámenia rozhodnutia komisii;

…

9. prípadne vážne skutočnosti, ktoré preukazujú, že advokát, lekár alebo novinár sa osobne a aktívne podieľa alebo podieľal na vzniku alebo vyvolaní hroziaceho nebezpečenstva;

10. v prípade, ak sa uplatní článok 18/8, odôvodnenie dĺžky obdobia, ktorého sa týka zber údajov;

…

(8) Vedúci útvaru ukončí uplatňovanie osobitnej metódy, ak zaniklo hroziace nebezpečenstvo, ktoré ju odôvodňuje, ak táto metóda už nie je užitočná pre dosiahnutie cieľa, pre ktorý sa uplatnila, alebo ak konštatoval nezákonnosť. O svojom rozhodnutí bezodkladne informuje komisiu.“

14. Článok 18/8 zákona z roku 1998 znie takto:

„(1) Spravodajské a bezpečnostné služby môžu v záujme plnenia svojich úloh, v prípade potreby po požiadaní operátora elektronickej komunikačnej siete alebo poskytovateľa elektronickej komunikačnej služby o technickú podporu na tento účel, pristúpiť alebo nariadiť, aby sa pristúpilo k:

1. zisteniu presnej polohy údajov o prenose dát na prostriedkoch elektronickej komunikácie, z ktorých alebo do ktorých smeruje alebo smerovala elektronická komunikácia;

2. lokalizácii pôvodu alebo cieľa elektronickej komunikácie.

…

(2) Čo sa týka uplatňovania metódy uvedenej odseku 1 na údaje uchovávané na základe článku 126 [zákona z roku 2005], použijú sa tieto ustanovenia:

1. v prípade hroziaceho nebezpečenstva týkajúceho sa činnosti, ktorá môže súvisieť so zločineckými organizáciami alebo so škodlivými sektárskymi organizáciami, môže vedúci útvaru vo svojom rozhodnutí vyžiadať údaje len za obdobie šiestich mesiacov pred vydaním rozhodnutia;

2. v prípade iného hroziaceho nebezpečenstva, než je hroziace nebezpečenstvo uvedené v bodoch 1 a 3, môže vedúci útvaru vo svojom rozhodnutí vyžiadať údaje za obdobie deviatich mesiacov pred vydaním rozhodnutia;

3. v prípade hroziaceho nebezpečenstva týkajúceho sa činnosti, ktorá môže súvisieť s terorizmom alebo extrémizmom, môže vedúci útvaru vo svojom rozhodnutí vyžiadať údaje za obdobie dvanástich mesiacov pred vydaním rozhodnutia. …“

II. Skutkový stav a položené prejudiciálne otázky

15. Cour constitutionnelle (Ústavný súd) rozsudkom z 11. júna 2015[14] vyhlásil nové znenie článku 126 zákona z roku 2005 za neplatné z tých istých dôvodov, ktoré viedli Súdny dvor k vyhláseniu smernice 2006/24 za neplatnú v rozsudku Digital Rights.

16. Vnútroštátny zákonodarca vzhľadom na uvedené rozhodnutie o neplatnosti schválil (ešte pred vydaním rozsudku Tele 2 Sverige a Watson) zákon z 29. mája 2016.

17. VZ a i., Ordre des barreaux francophones et germanophone (ďalej len „Ordre des barreaux“), Liga voor Mensenrechten ASBL (ďalej len „LMR“), Ligue des Droits de l’Homme ASBL (ďalej len „LDH“) a Académie Fiscale ASBL (ďalej len „Académie Fiscale“) podali na vnútroštátnom súde viaceré návrhy na vyhlásenie uvedeného zákona za protiústavný, pričom v podstate tvrdili, že tento zákon ide nad rámec toho, čo je prísne nevyhnutné, a nestanovuje dostatočné záruky ochrany.

[14] Rozsudok č. 84/2015, *Moniteur belge* z 11. augusta 2015.

18. Za týchto okolností Cour constitutionnelle (Ústavný súd) položil Súdnemu dvoru nasledujúce otázky:

„1. Má sa článok 15 ods. 1 smernice 2002/58/ES v spojení s právom na bezpečnosť zaručeným článkom 6 Charty základných práv Európskej únie [ďalej len ‚Charta'] a s právom na rešpektovanie osobných údajov, ktoré zaručujú články 7 a 8 a článok 52 ods. 1 Charty…, vykladať v tom zmysle, že bráni vnútroštátnej právnej úprave, o akú ide v konaní vo veci samej, ktorá ukladá operátorom a poskytovateľom elektronických komunikačných služieb všeobecnú povinnosť uchovávať údaje o prenose dát a polohe v zmysle smernice 2002/58/ES, ktoré tieto subjekty vytvárajú alebo spracúvajú v rámci poskytovania takýchto služieb, pričom cieľom tejto vnútroštátnej právnej úpravy nie je len vyšetrovanie, odhaľovanie a stíhanie závažných trestných činov, ale aj zaručenie národnej bezpečnosti, obrany územia a verejnej bezpečnosti, vyšetrovanie, odhaľovanie a stíhanie menej závažných trestných činov alebo zabránenie nepovolenému používaniu elektronických komunikačných systémov alebo dosiahnutie iného cieľa uvedeného v článku 23 ods. 1 [nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov) (Ú. v. EÚ L 119, 2016, s. 1)], a ktorá je navyše podmienená zárukami spresnenými v tejto právnej úprave, pokiaľ ide o uchovávanie údajov a prístup k nim?

2. Má sa článok 15 ods. 1 smernice 2002/58/ES v spojení s článkami 4, 7, 8, 11 a článkom 52 ods. 1 Charty… vykladať v tom zmysle, že bráni vnútroštátnej právnej úprave, o akú ide v konaní vo veci samej, ktorá ukladá operátorom a poskytovateľom elektronických komunikačných služieb všeobecnú povinnosť uchovávať údaje o prenose dát a polohe v zmysle smernice 2002/58/ES, ktoré tieto subjekty vytvárajú alebo spracúvajú v rámci poskytovania takýchto služieb, ak je cieľom tejto právnej úpravy najmä plniť pozitívne záväzky, ktoré orgánu vyplývajú z článkov 4 a 8 Charty a ktoré spočívajú vo vytvorení právneho rámca, ktorý umožní účinné vyšetrovanie a účinné potláčanie sexuálneho zneužívania maloletých osôb a tiež umožní skutočne identifikovať páchateľa trestného činu, a to aj vtedy, ak sa využívajú prostriedky elektronickej komunikácie?

3. Ak by Cour constitutionnelle [Ústavný súd] na základe odpovedí na prvú alebo druhú prejudiciálnu otázku dospel k záveru, že napadnutý zákon porušuje jednu alebo viaceré povinnosti vyplývajúce z ustanovení uvedených v týchto otázkach, mohol by dočasne zachovať účinky [sporného zákona], aby tak zabránil vzniku právnej neistoty a umožnil použitie v minulosti zhromaždených a uchovávaných údajov na účely stanovené zákonom?"

III. Konanie na Súdnom dvore

19. Návrh na začatie prejudiciálneho konania bol doručený do kancelárie Súdneho dvora 2. augusta 2018.

20. Písomné pripomienky predložili VZ a i., Académie Fiscale, LMR, LDH, Ordre des barreaux, Fondation pour Enfants Disparus et Sexuellement Exploités (Child Focus), nemecká, belgická, britská, česká, cyperská, dánska, španielska, estónska, francúzska, maďarská, írska, holandská, poľská a švédska vláda, ako aj Komisia.

21. Dňa 9. septembra 2019 sa uskutočnilo pojednávanie, ktoré sa konalo spoločne s pojednávaniami vo veciach C-511/18, C-512/18 a C-623/17 a na ktorom boli zastúpení účastníci všetkých štyroch konaní, v ktorých boli podané návrhy na začatie prejudiciálneho konania, uvedené vlády a nórska vláda, ako aj Komisia a Európsky dozorný úradník pre ochranu údajov.

IV. Analýza

22. Prvá otázka v tomto prejudiciálnom konaní sa v podstate zhoduje s otázkami prejednávanými vo veciach C-511/18 a C-512/28. Od týchto otázok sa však líši, pokiaľ ide o ciele, ktoré sleduje vnútroštátna právna úprava: týmito cieľmi nie je len boj proti terorizmu a proti najzávažnejším formám trestnej činnosti alebo zaručenie národnej bezpečnosti, ale aj „obrana územia, verejná bezpečnosť, vyšetrovanie, odhaľovanie a stíhanie menej závažných trestných činov“ a všeobecne ktorýkoľvek z cieľov uvedených v článku 23 ods. 1 nariadenia 2016/679.

23. Druhá otázka nadväzuje na prvú otázku, pričom dopĺňa ju v tom zmysle, že vnútroštátny súd sa pýta, či pozitívne záväzky, ktoré má verejná moc, pokiaľ ide o vyšetrovanie a sankcionovanie sexuálneho zneužívania maloletých osôb, môžu odôvodniť sporné opatrenia.

24. Tretia otázka sa kladie pre prípad, že by bol vnútroštátny predpis nezlučiteľný s právom Únie. Vnútroštátny súd chce vedieť, či by v takom prípade mohol dočasne zachovať účinky zákona z 29. mája 2016.

25. Pri rozbore týchto otázok v prvom rade preskúmam uplatniteľnosť smernice 2002/58, pričom v tejto súvislosti odkážem na svoje návrhy v ďalších z týchto prejudiciálnych konaní. V druhom rade opíšem najdôležitejšie závery vyplývajúce z judikatúry Súdneho dvora v tejto oblasti a možnosti jej rozpracovania. Napokon sa budem zaoberať odpoveďou na každú z prejudiciálnych otázok.

A. Uplatniteľnosť smernice 2002/58

26. Tak ako v ďalších troch prejudiciálnych konaniach, aj v tomto prejudiciálnom konaní bola spochybnená uplatniteľnosť smernice 2002/58. Keďže členské štáty majú na túto otázku rovnaký názor, v tejto súvislosti odkazujem na návrhy vo veciach C-511/18 a C-512/18 [15].

[15] Bod 40 a nasl.

B. Judikatúra Súdneho dvora týkajúca sa uchovávania osobných údajov a prístupu orgánov verejnej moci k nim v rámci smernice 2002/58

1. Zásada dôvernosti komunikácie a súvisiacich údajov

27. Ustanovenia smernice 2002/58 „spodrobňujú a dopĺňajú“ smernicu 95/46/ES [16] s cieľom dosiahnuť vysokú úroveň ochrany osobných údajov v súvislosti s poskytovaním elektronických komunikačných služieb [17].

28. V článku 5 ods. 1 smernice 2002/58 sa uvádza, že členské štáty musia vo svojich vnútroštátnych právnych predpisoch zabezpečiť dôvernosť správ prenášaných pomocou verejnej komunikačnej siete a verejne dostupných elektronických komunikačných sietí, ako aj dôvernosť príslušných údajov o prenose dát.

29. Z dôvernosti komunikácie okrem iného (článok 5 ods. 1 druhá veta smernice 2002/58) vyplýva, že sa akýmkoľvek iným osobám než používateľom zakazuje bez súhlasu týchto používateľov uchovávať údaje o prenose dát týkajúce sa elektronickej komunikácie. Predmetom výnimiek sú „osoby oprávnené zákonom… a technické uchovávanie, ktoré je nevyhnutné na účely prenosu správy“. [18]

30. Účelom článkov 5 a 6 a článku 9 ods. 1 smernice 2002/58 je zachovať dôvernosť komunikácie a súvisiacich údajov a minimalizovať riziko zneužitia. Rozsah ich pôsobnosti treba posúdiť s ohľadom na odôvodnenie 30 tejto smernice, podľa ktorého „systémy poskytovania elektronických komunikačných sietí a služieb by mali byť konštruované tak, aby bol obmedzený počet nevyhnutných osobných údajov na *minimum*“. [19]

31. Pokiaľ ide o tieto údaje, možno rozlíšiť:

– údaje o prenose dát, ktorých spracúvanie a uchovávanie je povolené len v rozsahu a na obdobie potrebné na účely fakturácie služieb, ich marketingu alebo poskytovania služieb s pridanou hodnotou (článok 6 smernice 2002/58). Po uplynutí tejto doby sa údaje, ktoré boli spracúvané a uchovávané, musia vymazať alebo anonymizovať; [20]

– údaje o *polohe* iné, než sú údaje o prenose dát, ktoré sa môžu spracovávať len za určitých podmienok a potom, ako boli anonymizované, alebo po získaní súhlasu užívateľov alebo účastníkov (článok 9 ods. 1 smernice 2002/58). [21]

16 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). Pozri článok 1 ods. 2 smernice 2002/58. Smernica 95/46 bola s účinnosťou od 25. mája 2018 zrušená nariadením 2016/679. Pokiaľ teda smernica 2002/58 odkazuje na smernicu 95/46 alebo nestanovuje vlastné pravidlá, je nevyhnutné zohľadniť ustanovenia uvedeného nariadenia (pozri článok 94 ods. 1 a 2 nariadenia 2016/679).

17 Rozsudok Tele2 Sverige a Watson, body 82 a 83.

18 Tamže, bod 85 a citovaná judikatúra.

19 Tamže, bod 87. Kurzívou zvýraznil generálny advokát.

20 Tamže, bod 86 a citovaná judikatúra.

21 Tamže, bod 86 *in fine*.

2. Obmedzujúca doložka uvedená v článku 15 ods. 1 smernice 2002/58

32. Článok 15 ods. 1 smernice 2002/58 dovoľuje členským štátom „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“ uvedenej smernice.

33. Každé obmedzenie musí predstavovať „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 elektronického komunikačného systému podľa článku 13 ods. 1 smernice [95/46]“.

34. Uvedený zoznam cieľov je taxatívny:[22] napríklad („medzi iným“) sú dovolené „legislatívne opatrenia umožňujúce zadržanie [uchovávanie – *neoficiálny preklad*] údajov na limitované obdobie, oprávnené z dôvodov stanovených v tomto odseku“.

35. V každom prípade „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“. Článok 15 ods. 1 smernice 2002/58 sa má preto vykladať v spojení so základnými právami zaručenými Chartou.[23]

36. Spomedzi týchto práv uznaných v Charte Súdny dvor – v rozsahu relevantnom pre prejednávanú vec – spomenul právo na súkromie (článok 7), právo na ochranu osobných údajov (článok 8) a právo na slobodu prejavu (článok 11).[24]

37. Súdny dvor rovnako zdôraznil – ako pravidlo výkladu článku 15 ods. 1 smernice 2002/58, ktorý podal –, že obmedzenia povinnosti zabezpečiť dôvernosť komunikácie a súvisiacich údajov o prenose dát sa majú vykladať reštriktívne.

38. Konkrétne nesúhlasil s tým, „že výnimka z tejto zásadnej povinnosti, a najmä výnimka zo zákazu uchovávať tieto údaje stanovená v článku 5 tejto smernice, sa stane pravidlom, pretože v takom prípade by došlo k zbaveniu tohto ustanovenia veľkej časti jeho rozsahu pôsobnosti“.[25]

39. Tieto dve konštatovania považujem za rozhodujúce pre pochopenie, prečo Súdny dvor považoval všeobecné a nediferencované uchovávanie údajov o prenose dát a polohe týkajúcich sa elektronickej komunikácie za nezlučiteľné so smernicou 2002/58.

40. Súdny dvor týmto rozhodnutím len „prísne“[26] uplatnil kritérium proporcionality, ktoré použil už predtým:[27] „ochrana základného práva na rešpektovanie súkromného života na úrovni Únie vyžaduje, aby výnimky a obmedzenia v súvislosti s ochranou osobných údajov nepôsobili nad rámec toho, čo je prísne nevyhnutné“[28].

22 Tamže, bod 90.

23 Tamže, bod 91 a citovaná judikatúra.

24 Tamže, bod 93 a citovaná judikatúra.

25 Tamže, bod 89.

26 Použitie tejto príslovky v bode 95 rozsudku Tele2 Sverige a Watson vychádza z odôvodnenia 11 smernice 2002/58.

27 Rozsudok Digital Rights, bod 48: „vzhľadom na dôležitú úlohu, ktorú na jednej strane zohráva ochrana osobných údajov so zreteľom na základné právo rešpektovania súkromného života, a na druhej strane, rozsah a závažnosť zásahu do tohto práva, ktorý obsahuje smernica 2006/24, je voľná úvaha normotvorcu Únie obmedzená, takže treba pristúpiť k prísnej kontrole“.

28 Rozsudok Tele2 Sverige a Watson, bod 96 a citovaná judikatúra.

3. Primeranosť uchovávania údajov

a) Neprimeranosť všeobecného a nediferencovaného uchovávania

41. Súdny dvor uznal, že boj proti závažnej trestnej činnosti, najmä proti organizovanému zločinu a terorizmu, má prvoradý význam na zabezpečenie verejnej bezpečnosti a jeho účinnosť môže vo veľkej miere závisieť od použitia moderných vyšetrovacích technológií. Dodal však, že „takýto cieľ všeobecného záujmu, nech je akokoľvek zásadný, nemôže sám osebe odôvodniť to, aby sa opatrenie uchovávania zavedené smernicou 2006/24 považovalo za nevyhnutné na účely uvedeného boja“.[29]

42. Pri rozhodovaní o tom, či takéto opatrenie bolo obmedzené na to, čo je prísne nevyhnutné, Súdny dvor predovšetkým zdôraznil mimoriadnu závažnosť zásahu do základných práv zakotvených v článkoch 7 a 8 Charty, ktorý spôsobovalo toto opatrenie.[30] Táto mimoriadna závažnosť vyplývala práve z toho, že vnútroštátne právne predpisy stanovovali „všeobecné a nediferencované uchovávanie *všetkých údajov o prenose dát a polohe všetkých účastníkov a registrovaných užívateľov, týkajúce sa všetkých prostriedkov elektronickej komunikácie*, a vyžad[ovali] od poskytovateľov elektronických komunikačných služieb uchovávať tieto údaje *priebežne a systematicky, a to bez výnimky*“.[31]

43. Zásah do života občanov, ktorý spôsobovalo uvedené opatrenie, je vyjadrený v týchto konštatovaniach Súdneho dvora týkajúcich sa účinkov uchovávania údajov.

Tieto údaje[32]

– „umožňujú zistenie a identifikáciu zdroja komunikácie a adresáta komunikácie, určenie dátumu, času, trvania a typu komunikácie, identifikáciu komunikačného zariadenia užívateľa, ako aj určenie polohy mobilného komunikačného zariadenia“;[33]

– „z týchto údajov predovšetkým vyplýva, s kým a akým spôsobom účastník alebo registrovaný užívateľ komunikoval, ako aj čas komunikácie a miesto, z ktorého prebiehala. Okrem toho tieto údaje umožňujú zistiť, ako často účastník alebo registrovaný užívateľ komunikoval s určitými osobami v danom období“;[34]

– „zo všetkých týchto údajov možno vyvodiť presné závery týkajúce sa súkromného života osôb, ktorých údaje boli uchovávané, ako ich každodenné zvyklosti, miesta ich trvalého alebo prechodného pobytu, denné alebo iné presuny, vykonávané činnosti, spoločenské vzťahy týchto osôb a spoločenské kruhy, v ktorých sa pohybujú“;[35]

29 Rozsudok Digital Rights, bod 51. Pozri v tom istom zmysle rozsudok Tele2 Sverige a Watson, bod 103.

30 Rozsudky Digital Rights, bod 65, a Tele2 Sverige a Watson, bod 100.

31 Rozsudok Tele2 Sverige a Watson, bod 97. Kurzívou zvýraznil generálny advokát.

32 Medzi ktoré patrí meno a adresa účastníka alebo registrovaného užívateľa, telefónne číslo volajúceho a číslo volaného, ako aj IP adresa pre internetové služby.

33 Rozsudok Tele2 Sverige a Watson, bod 98.

34 Tamže, bod 98.

35 Tamže, bod 99.

– „takéto údaje poskytujú prostriedky na stanovenie… profilu dotknutých osôb, čo je rovnako citlivá informácia, pokiaľ ide o právo na rešpektovanie súkromného života, ako samotný obsa[h] komunikácií“ [36].

44. Tento zásah môže navyše „v povedomí dotknutých osôb vyvolať pocit, že ich súkromný život je predmetom neustáleho sledovania“, lebo „uchovávanie údajov sa uskutočňuje bez toho, aby používatelia elektronických komunikačných služieb boli o tom informovaní“. [37]

45. Vzhľadom na rozsah tohto zásahu opatrenie spočívajúce v uchovávaní údajov s týmito znakmi možno odôvodniť výhradne bojom proti závažnej trestnej činnosti. [38] Toto opatrenie sa však nemôže zmeniť na všeobecné pravidlo, lebo „podľa systému zavedeného smernicou 2002/58 sa vyžaduje, aby uchovávanie údajov bolo výnimkou“. [39]

46. Zo skutočnosti, že posudzované opatrenie nestanovovalo „žiadne rozlíšenie, obmedzenie alebo výnimku na základe sledovaného cieľa“ [40] a „nevyžad[ovalo] nijakú súvislosť medzi údajmi, ktorých uchovávanie stanov[ovalo], a hrozbou pre verejnú bezpečnosť“, navyše vyplývali dva znaky: [41]

– na jednej strane toto opatrenie sa globálne týkalo „všetkých osôb používajúcich elektronické komunikačné služby bez toho, aby sa tieto osoby aspoň nepriamo nachádzali v situácii, ktorá by mohla viesť k trestnému stíhaniu. … Navyše nestanov[ovalo] žiadnu výnimku, takže sa uplatň[ovalo] aj na osoby, ktorých komunikácia podľa pravidiel vnútroštátneho práva podlieha služobnému tajomstvu“; [42]

– na druhej strane nebolo „… obmedzen[é] 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“. [43]

47. Za týchto podmienok posudzované vnútroštátne právne predpisy išli nad rámec toho, čo je prísne nevyhnutné. Preto nebolo možné považovať ich za odôvodnené 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. [44]

b) Uskutočniteľnosť cieleného uchovávania údajov

48. Súdny dvor uznal, že právu Únie neodporujú vnútroštátne právne predpisy, ktoré „preventívne umožňuj[ú], aby sa *cielene uchovávali* údaje o prenose dát a polohe na účely boja proti závažnej trestnej činnosti“. [45]

36 Tamže, bod 99 *in fine*.

37 Tamže, bod 100.

38 Tamže, bod 102.

39 Tamže, bod 104.

40 Tamže, bod 105.

41 Tamže, bod 106.

42 Tamže, bod 105.

43 Tamže, bod 106.

44 Tamže, bod 107.

45 Tamže, bod 108. Kurzívou zvýraznil generálny advokát.

49. Prípustnosť tohto cieleného uchovávania údajov je podmienená tým, že toto uchovávanie „bude, pokiaľ ide o kategórie uchovávaných údajov, príslušné komunikačné prostriedky, dotknuté osoby, ako aj dĺžku doby uchovávania, obmedzené na to, čo je prísne nevyhnutné“.

50. Pravidlá na určenie, kedy sú uvedené podmienky splnené, vyplývajúce z rozsudku Tele 2 Sverige a Watson, nie sú (zrejme nemohli byť) taxatívne a sú sformulované skôr všeobecne. Na ich dodržanie musia členské štáty:

– stanoviť jasné a presné pravidlá upravujúce rozsah a uplatnenie takého opatrenia na uchovávanie údajov; [46]

– určiť „objektívn[e] kritéri[á], ktoré zodpovedajú vzťahu medzi uchovávanými údajmi a sledovaným cieľom“, [47] a

– vychádzať z „objektívnych skutočnost[í], ktoré umožňujú definovať určitý okruh osôb z radov verejnosti, ktorých údaje môžu aspoň nepriamo súvisieť so závažnou trestnou činnosťou, podporiť určitým spôsobom boj proti závažnej trestnej činnosti alebo zabrániť vážnemu ohrozeniu verejnej bezpečnosti“. [48]

51. V súvislosti s týmito objektívnymi skutočnosťami Súdny dvor uvádza ako príklad možnosť použiť na vymedzenie verejnosti a potenciálne dotknutých situácií geografické kritérium. Domnievam sa, že účelom uvedenia spomenutého kritéria, ku ktorému sa kriticky vyjadrili niektoré členské štáty, nie je obmedziť zoznam prípustných faktorov cieleného uchovávania len na toto kritérium.

4. Primeranosť prístupu k údajom

a) Rozsudok Tele2 Sverige a Watson

52. Súdny dvor posudzuje *prístup* vnútroštátnych orgánov k údajom nezávisle od rozsahu povinnosti *uchovávania* uloženej poskytovateľom elektronických komunikačných služieb, najmä nezávisle od všeobecného alebo osobitného charakteru uchovávania týchto údajov. [49]

53. Aj keď je totiž účelom uchovávania uľahčiť neskorší prístup k údajom, uchovávanie aj prístup môžu spôsobiť odlišné porušenia základných práv chránených Chartou. Toto rozlišovanie však neznamená, že niektoré z úvah týkajúcich uchovávania nemožno uplatniť aj na prístup k uchovávaným údajom.

54. V tomto zmysle prístup:

– „musí skutočne a výlučne zodpovedať jednému z týchto cieľov“ uvedených v článku 15 ods. 1 prvej vete smernice 2002/58. Závažnosť zásahu tiež musí zodpovedať sledovanému cieľu. Ak sa

[46] Tamže, bod 109. Musia najmä uvádzať „za akých podmienok môže byť opatrenie na uchovávanie údajov preventívne prijaté, čím sa zabezpečí, že také opatrenie sa obmedzí na to, čo je prísne nevyhnutné“.

[47] Tamže, bod 110.

[48] Tamže, bod 111.

[49] Tamže, bod 113.

tento zásah považuje za závažný, možno ho odôvodniť jedine bojom proti závažnej trestnej činnosti;[50]

– možno povoliť len v rámci toho, čo je prísne nevyhnutné.[51] Legislatívne opatrenia navyše musia stanoviť „jasné a presné pravidlá uvádzajúce, za akých okolností a podmienok musia poskytovatelia elektronických komunikačných služieb poskytnúť prístup príslušným vnútroštátnym orgánom k uchovávaným údajom. Okrem toho takéto opatrenie musí byť podľa vnútroštátneho práva právne záväzné“;[52]

– vnútroštátne právne úpravy konkrétnejšie musia stanoviť „hmotnoprávne a procesnoprávne podmienky prístupu príslušných vnútroštátnych orgánov k uchovávaným údajom“.[53]

55. Z vyššie uvedeného možno vyvodiť, že „všeobecný prístup ku všetkým uchovávaným údajom, bez ohľadu na akúkoľvek spojitosť – čo i len nepriamu – so sledovaným účelom nemožno považovať za obmedzený na prísne nevyhnutné“.[54]

56. Podľa Súdneho dvora „dotknutá vnútroštátna právna úprava sa musí zakladať na objektívnych kritériách s cieľom určiť okolnosti a podmienky, za akých sa má poskytnúť prístup príslušným vnútroštátnym orgánom k uchovávaným údajom účastníkov alebo registrovaných užívateľov“.[55] Z tohto pohľadu „možno taký prístup v súvislosti s cieľom boja proti kriminalite v zásade poskytnúť len k *údajom osôb podozrivých z prípravy, páchania alebo zo spáchania závažného trestného činu, ako aj tých, ktoré sa takým či onakým spôsobom podieľali na takom trestnom čine*“.[56]

57. Inak povedané, vnútroštátne predpisy, ktoré poskytujú príslušným vnútroštátnym orgánom prístup k uchovávaným údajom, musia mať dostatočne obmedzený rozsah. Musí existovať súvislosť medzi dotknutými osobami a sledovaným cieľom, aby sa prístup nevzťahoval na značný počet osôb alebo dokonca na všetky osoby, na všetky prostriedky elektronickej komunikácie a na všetky uchovávané údaje.

58. Tieto pravidlá však možno za určitých okolností zmierniť. Súdny dvor má na mysli „osobitn[é] okolnost[i], ako sú okolnosti, za akých životne dôležité záujmy národnej bezpečnosti, obrany alebo verejnej bezpečnosti sú ohrozené teroristickými aktivitami“. Za takých okolností „možno… poskytnúť prístup aj k údajom iných osôb, pokiaľ existujú objektívne skutočnosti, na základe ktorých sa možno domnievať, že tieto údaje môžu v konkrétnom prípade účinne prispieť k boju proti takýmto činnostiam“.[57]

59. Toto vysvetlenie Súdneho dvora umožňuje členským štátom zaviesť osobitný režim širšieho prístupu k údajom, ak je to výnimočne nevyhnutné na boj proti hrozbám pre základné záujmy štátu (národná bezpečnosť, obrana a verejná bezpečnosť)[58], ktorý by zahŕňal aj osoby, ktoré sú len nepriamo spojené s uvedenými rizikami.

50 Tamže, bod 115.

51 Tamže, bod 116.

52 Tamže, bod 117.

53 Tamže, bod 118.

54 Tamže, bod 119.

55 Tamže.

56 Tamže. Kurzívou zvýraznil generálny advokát.

57 Tamže.

58 Okrem teroristických aktivít by uvedenú výnimočnosť mohli odôvodniť iné situácie, ako je rozsiahly počítačový útok na kľúčové zariadenia štátu alebo hrozba súvisiaca so šírením jadrových zbraní.

60. Prístup vnútroštátnych orgánov k uchovávaným údajom musí bez ohľadu na ich druh podliehať trom podmienkam:

– je potrebné, aby podliehal „v zásade – s výnimkou riadne odôvodnených naliehavých prípadov – predchádzajúcemu preskúmaniu zo strany súdu alebo nezávislého správneho orgánu“. Rozhodnutie tohto súdu alebo orgánu sa musí prijať „po odôvodnenej žiadosti týchto orgánov podanej v rámci konania týkajúceho sa predchádzania trestným činom, ich odhaľovania a stíhania“; [59]

– je dôležité, aby „príslušné vnútroštátne orgány, ktorým bol udelený prístup k uchovávaným údajom, informovali dotknuté osoby v rámci uplatniteľných vnútroštátnych konaní od okamihu, keď toto oznámenie nemôže ohroziť vyšetrovanie týchto orgánov“; [60]

– členské štáty musia prijať pravidlá týkajúce sa bezpečnosti a ochrany údajov, ktorými disponujú poskytovatelia elektronických komunikačných služieb, aby sa zabránilo neoprávnenému používaniu a nezákonnému prístupu k údajom. [61]

b) Rozsudok Ministerio Fiscal

61. Predmetom uvedenej veci bola otázka, či je s článkom 15 ods. 1 smernice 2002/58 v spojení v článkami 7 a 8 Charty zlučiteľný vnútroštátny predpis, ktorý stanovuje, že príslušné orgány majú prístup k údajom týkajúcim sa občianskej totožnosti držiteľov určitých SIM kariet.

62. Súdny dvor rozhodol, že článok 15 ods. 1 prvá veta smernice 2002/58 neobmedzuje cieľ prevencie, vyšetrovania, odhaľovania a stíhania trestných činov iba na boj proti závažným trestným činom, ale vzťahuje sa na „trestné činy“ vo všeobecnosti. [62]

63. Dodal, že prístup príslušných vnútroštátnych orgánov k údajom je odôvodnený len v prípade, ak závažnosť zásahu zodpovedá závažnosti predmetných trestných činov. V dôsledku toho:

– „závažný zásah“ možno „odôvodniť iba cieľom boja proti kriminalite, ktorá musí byť tiež považovaná za ‚závažnú‘“; [63]

– naopak, „ak zásah, ktorý takýto prístup v sebe zahŕňa, nie je závažný, uvedený prístup môže byť odôvodnený cieľom prevencie, vyšetrovania, odhaľovania a stíhania ‚trestných činov‘ vo všeobecnosti“. [64]

64. Na základe tohto predpokladu – a na rozdiel od toho, k čomu došlo v rozsudku Tele2 Sverige a Watson – Súdny dvor nepovažoval zásah do práv chránených článkami 7 a 8 Charty za „závažný“, lebo jediným cieľom žiadosti o prístup bola „identifikácia držiteľov SIM kariet aktivovaných počas obdobia dvanástich dní s kódom IMEI odcudzeného mobilného telefónu“. [65]

[59] Rozsudok Tele2 Sverige a Watson, bod 120.

[60] Tamže, bod 121.

[61] Tamže, bod 122.

[62] Rozsudok Ministerio Fiscal, bod 53.

[63] Tamže, bod 56.

[64] Tamže, bod 57.

[65] Tamže, bod 59. Išlo o prístup „k telefónnym číslam zodpovedajúcim týmto SIM kartám, ako aj k údajom týkajúcim sa občianskej totožnosti držiteľov uvedených kariet, ako sú ich meno, priezvisko a prípadne adresa. Naopak, tieto údaje sa netýkajú, ako to potvrdili španielska vláda a prokuratúra na pojednávaní, komunikácií uskutočnených s odcudzeným mobilným telefónom ani jeho lokalizácie“.

65. S cieľom poukázať na menšiu závažnosť tohto zásahu vysvetlil, že „údaje, ktorých sa týka žiadosť o prístup dotknutá vo veci samej, umožňujú len prepojiť počas určitého obdobia SIM kartu alebo SIM karty aktivované s odcudzeným mobilným telefónom s občianskou totožnosťou držiteľov týchto SIM kariet. Bez porovnania s údajmi vzťahujúcimi sa na komunikácie uskutočnené s uvedenými SIM kartami a lokalizačnými údajmi tieto údaje neumožňujú dozvedieť sa ani dátum, hodinu, trvanie a adresátov komunikácií uskutočnených s dotknutou SIM kartou alebo SIM kartami a ani miesta, kde k týmto komunikáciám došlo alebo ich frekvenciu s určitými osobami počas daného obdobia. Uvedené údaje teda neumožňujú vyvodiť presné závery o súkromnom živote osôb, ktorých údaje sú dotknuté“. [66]

66. Vo veci, v ktorej bol vydaný rozsudok Ministerio Fiscal, nebolo potrebné rozhodnúť, či sprístupňované osobné údaje boli uchovávané poskytovateľmi elektronických komunikačných služieb v súlade s podmienkami uvedenými v článku 15 ods. 1 smernice 2002/58 v spojení v článkami 7 a 8 Charty. [67] Súdny dvor sa v uvedenom rozsudku nezaoberal ani otázkou, či boli splnené ostatné podmienky prístupu vyplývajúce z uvedeného článku.

67. Zo znenia rozsudku Ministerio Fiscal preto nemožno vyvodiť nijakú zmenu v judikatúre Súdneho dvora týkajúcej sa nezlučiteľnosti vnútroštátnych predpisov, ktoré povoľujú všeobecné a nediferencované uchovávanie údajov v zmysle rozsudku Tele2 Sverige a Watson, s právom Únie.

68. Domnievam sa však, že Súdny dvor tým, že uznal platnosť režimu prístupu obmedzeného na niektoré osobné údaje (týkajúce sa občianskej totožnosti držiteľov SIM kariet), implicitne uznal možnosť, aby poskytovatelia služby uchovávali tieto údaje.

C. Hlavné výhrady voči judikatúre Súdneho dvora

69. Tak vnútroštátny súd, ako aj väčšina členských štátov, ktoré predložili pripomienky, vyzývajú Súdny dvor, aby objasnil, upravil či dokonca prehodnotil viaceré aspekty svojej judikatúry v tejto oblasti, voči ktorej smerujú ich výhrady.

70. Väčšina uvedených – nepriamych či priamych – výhrad už bola vyjadrená v dôsledku rozsudku Digital Rights a zamietnutá v rozsudku Tele 2 Sverige a Watson. Tieto výhrady sa v súčasnosti znova objavujú s cieľom poukázať v podstate na to, že by postačovali prísne pravidlá týkajúce sa prístupu k údajom, ktorými disponujú poskytovatelia elektronických komunikačných služieb, ktoré by mohli určitým spôsobom kompenzovať závažnosť zásahu, ktorý predstavuje všeobecné a nediferencované uchovávanie týchto údajov.

71. Vo viacerých z uvedených výhrad sa tiež zdôrazňuje potreba prijať skutočne účinné opatrenia v boji proti vážnym hrozbám pre bezpečnosť a proti trestnej činnosti vo všeobecnosti, pričom sa žiada, aby Súdny dvor vzal do úvahy právo na bezpečnosť (článok 6 Charty), ako aj priestor na voľnú úvahu členských štátov pri ochrane národnej bezpečnosti. Niekedy sa tiež namieta, že Súdny dvor nezvážil preventívny charakter zásahu bezpečnostných a spravodajských služieb.

66 Tamže, bod 60.

67 Rozsudok Ministerio Fiscal, bod 49.

D. Moje posúdenie uvedených výhrad a prípadných úprav judikatúry Súdneho dvora

72. Domnievam sa, že Súdny dvor by mal zotrvať na principiálnom stanovisku, ku ktorému dospel vo svojich skorších rozsudkoch: všeobecná a nediferencovaná povinnosť uchovávať všetky údaje o prenose dát a polohe všetkých účastníkov a registrovaných užívateľov neprimerane porušuje základné práva chránené článkami 7, 8 y 11 Charty.

73. Naopak vnútroštátne právne predpisy, ktoré by stanovovali primerané obmedzenia uchovávania niektorých z týchto údajov, vytvorených v rámci poskytovania elektronických komunikačných služieb, by mohli byť zlučiteľné s právom Únie. Rozhodujúce je teda *obmedzené uchovávanie* týchto údajov.

74. Z dôvodov, ktoré uvediem nižšie, by uvedeným obmedzeným uchovávaním nemalo byť len uchovávanie, ktoré sa vzťahuje na určitú zemepisnú oblasť alebo na určitú kategóriu konkrétnych osôb: diskusie o týchto kritériách uchovávania svedčia o tom, že by buď mohli byť nerealizovateľné alebo neúčinné z hľadiska sledovaných cieľov, alebo by sa dokonca mohli zmeniť na zdroj diskriminácie.

75. Na úvod poznamenávam, že nesúhlasím s námietkou, ktorá presadzuje pravidlo „rozsiahlejšie uchovávanie, ale obmedzenejší prístup“. Úvahy Súdneho dvora, s ktorými súhlasím, spočívajú v tom, že uchovávanie a prístup k údajom predstavujú dva odlišné typy zásahu. Aj keď má uchovávanie údajov zmysel so zreteľom na možný neskorší prístup príslušných orgánov, každý z týchto zásahov sa musí odôvodniť samostatne, prostredníctvom osobitného preskúmania z hľadiska sledovaného cieľa.

76. Vnútroštátny systém, ktorý stanovuje všeobecné a nediferencované uchovávanie údajov, preto nemožno odôvodniť na základe toho, že príslušné predpisy zároveň stanovujú prísne hmotnoprávne a procesnoprávne podmienky prístupu k týmto údajom.

77. Musia teda existovať predpisy, ktoré konkrétne súvisia s uchovávaním údajov a ktoré stanovujú určité podmienky tohto uchovávania s cieľom zabrániť tomu, aby bolo všeobecné a nediferencované. Len tak sa zaručí ich zlučiteľnosť s článkom 15 ods. 1 smernice 2002/58 v spojení s článkami 7, 8 a 11 a článkom 52 ods. 1 Charty.

78. Práve tento postup navyše použili pracovné skupiny združené v rámci Rady na vymedzenie predpisov týkajúcich sa uchovávania a prístupu, ktoré sú zlučiteľné s judikatúrou Súdneho dvora, pri súbežnom skúmaní oboch typov zásahu. [68]

79. Pri uplatnení obmedzení na každý z týchto dvoch typov zásahov možno posúdiť, či ich prípadný kumulatívny účinok, spojený s primeranými zárukami, zmierňuje vplyv uchovávania údajov na základné práva chránené článkami 7, 8 a 11 Charty a zároveň zaručuje efektívnosť vyšetrovania.

80. Ak má tento systém chrániť uvedené práva, musí:

– stanovovať uchovávanie údajov, ktoré zahŕňa určité obmedzenia a rozdiely v závislosti od sledovaného cieľa;

[68] Členské štáty sú od roku 2017 členmi pracovnej skupiny, ktorej cieľom je prispôsobiť ich právne predpisy kritériám stanoveným v judikatúre Súdneho dvora týkajúcej sa tejto oblasti [Pracovná skupina pre výmenu informácií a ochranu údajov (DAPIX)].

– upravovať prístup k týmto údajom len v rozsahu, ktorý je prísne nevyhnutný na dosiahnutie sledovaného cieľa, a podlieha preskúmaniu zo strany súdu alebo nezávislého správneho orgánu.

81. Dôvodnosť, aby poskytovatelia elektronických komunikačných služieb uchovávali určité údaje, a to nielen na účely plnenia svojich zmluvných záväzkov voči užívateľom, sa súbežne s technickým pokrokom posilňuje. Ak by sa pripustilo, že toto uchovávanie je užitočné pre predchádzanie a boj proti trestnej činnosti (čo sa dá ťažko vyvrátiť[69]), nezdalo by sa logické obmedziť jeho rozsah len na využívanie údajov, ktoré operátori uchovávajú na vykonávanie svojej obchodnej činnosti, a to len počas doby nevyhnutnej na vykonávanie tejto činnosti.

82. Ak sa uzná, že povinnosť uchovávania údajov je – nad rámec údajov, ktoré môžu operátori uchovávať pre vlastné technické a obchodné potreby – užitočná pre ochranu národnej bezpečnosti a boj proti trestnej činnosti, je nevyhnutné vymedziť hranice tejto povinnosti.

83. Každý režim uchovávania musí prísne zodpovedať sledovanému cieľu, aby nemohol vyústiť do nediferencovaného uchovávania.[70] Tiež musí zabrániť tomu, aby zo súhrnu týchto údajov vyplynula *predstava* o dotknutej osobe (teda o jej obvyklých činnostiach a spoločenských vzťahoch) blízka alebo podobná predstave, ktorá by vznikla v prípade, ak by bol známy obsah komunikácie.

84. Na vyjasnenie určitých nedorozumení a nepochopení je dôležité vziať do úvahy, čo Súdny dvor *nekonštatoval* vo svojich rozsudkoch Digital Rigths a Tele2 Sverige a Watson. V týchto rozsudkoch nebola odmietnutá samotná existencia režimu uchovávania údajov ako účinného nástroja v boji proti trestnej činnosti. Naopak Súdny dvor uznal legitímnosť cieľa spočívajúceho v predchádzaní a potláčaní trestných činov, ako aj užitočnosť režimu uchovávania údajov pre dosiahnutie uvedeného cieľa.

85. Pripomínam, že Súdny dvor vtedy kategoricky odmietol možnosť, aby Únia alebo jej členské štáty s odvolaním sa na tento cieľ vyžadovali nediferencované uchovávanie *všetkých* údajov vytvorených v rámci poskytovania elektronických komunikačných služieb a všeobecný prístup k týmto údajom.

86. Preto je potrebné nájsť formy uchovávania údajov, vďaka ktorým nebude možné označiť uchovávanie údajov prívlastkami („všeobecné a nediferencované“), ktoré sú nezlučiteľné s ochranou vyžadovanou článkami 7, 8 a 11 Charty.

87. Jednou z uvedených foriem by bolo *cielené* uchovávanie údajov týkajúcich sa buď konkrétnej časti verejnosti (teoreticky časti verejnosti, ktorú spájajú s najzávažnejšími hrozbami určité, viac či menej priame väzby), alebo určitej zemepisnej oblasti.

88. Uvedený prístup však vyvoláva určité ťažkosti:

– identifikácia skupiny potenciálnych páchateľov by pravdepodobne bola nedostatočná, ak užívatelia využívajú anonymizačné postupy alebo falšujú svoju totožnosť. Výber týchto skupín by navyše mohol viesť k zavedeniu režimu všeobecného podozrenia týkajúceho sa niektorých častí obyvateľstva a v závislosti od použitého vzorca by sa mohol považovať za diskriminačný;

69 Určenie postupov vyšetrovania a posúdenie ich účinnosti v každom prípade spadá do voľnej úvahy členských štátov.

70 Rozsudok Digital Rights, bod 57, a rozsudok Tele2 Sverige a Watson, bod 105.

– výber podľa zemepisných kritérií (ktorý by bol účinný len vtedy, ak by sa netýkal veľmi malých území) vyvoláva tie isté problémy a tiež ďalšie problémy, ako to na pojednávaní uviedol Európsky dozorný úradník pre ochranu osobných údajov, keďže by mohol viesť k stigmatizácii určitých oblastí.

89. Okrem toho by mohol existovať určitý rozpor medzi preventívnym charakterom uchovávania zameraného na konkrétnu časť verejnosti alebo na určitú zemepisnú oblasť a skutočnosťou, že páchatelia, miesto ani čas spáchania trestných činov nie sú vopred známe.

90. V každom prípade nemožno vylúčiť, že sa nájdu vzorce cieleného uchovávania založené na uvedených kritériách, ktoré budú užitočné pre dosiahnutie vyššie opísaných cieľov. Prináleží zákonodarnej moci, aby v každom členskom štáte alebo v celej Únii určila tieto vzorce, ktoré budú v súlade s ochranou základných práv, ktoré zaručuje Súdny dvor.

91. Bolo by mylné domnievať sa, že cielené uchovávanie údajov týkajúcich sa konkrétnej časti verejnosti alebo určitej zemepisnej oblasti je jediným vzorcom, ktorý Súdny dvor považuje za zlučiteľný s článkom 15 ods. 1 smernice 2002/58 v spojení s článkami 7 a 8 Charty.

92. Zdôrazňujem, že je možné nájsť iné spôsoby cieleného uchovávania údajov okrem tých, ktoré sú zamerané na konkrétne skupiny osôb alebo zemepisné oblasti. K tomuto záveru v skutočnosti dospeli pracovné skupiny Rady, ktoré som spomenul vyššie: za prostriedky, ktoré treba preskúmať, považovali najmä obmedzenie kategórií uchovávaných údajov[71], pseudonymizáciu údajov[72], zavedenie obmedzených dôb uchovávania[73], vylúčenie určitých kategórií poskytovateľov elektronických komunikačných služieb[74], obnoviteľné povolenia na uchovávanie[75], povinnosť uchovávať uchovávané údaje v rámci Únie alebo systematickú a pravidelnú kontrolu záruk pred neoprávneným používaním údajov, ktoré ponúkajú poskytovatelia elektronických komunikačných služieb, vykonávanú nezávislým správnym orgánom.

93. Domnievam sa, že na zabezpečenie súladu s judikatúrou Súdneho dvora by sa malo uprednostniť dočasné uchovávanie niektorých *kategórií* údajov o prenose dát a polohe, ktoré budú obmedzené v závislosti od nevyhnutných bezpečnostných potrieb a ktoré ako celok neumožnia získať presný a podrobný obraz o živote dotknutých osôb.

71 Údaje, ktoré nie sú prísne nevyhnutné a objektívne potrebné na prevenciu a stíhanie trestných činov a ochranu verejnej bezpečnosti, by boli vyňaté z povinnosti uchovávania. Najmä by bolo potrebné v súlade so sledovaným cieľom určiť, ktoré typy údajov účastníkov, údajov o prenose dát a údajov o polohe by sa museli povinne uchovávať na dosiahnutie uvedeného cieľa. Osobitne by boli vyňaté údaje, ktoré sa nepovažujú za nevyhnutné pre vyšetrovanie trestných činov a rozhodovanie o nich.

72 Metóda, ktorou sa mená nahradia prezývkou, a tak sa údaje už neviažu na meno. Na rozdiel od anonymizácie pseudonymizácia umožňuje opäť spojiť údaje s menom dotknutej osoby.

73 Do úvahy prichádza preskúmať možnosť upraviť doby uchovávania podľa jednotlivých kategórií údajov s prihliadnutím na to, či vo väčšej alebo menšej miere zasahujú do súkromného života jednotlivcov. Okrem toho by sa malo stanoviť, ktoré údaje sa po uplynutí doby uchovávania natrvalo vymažú.

74 Dala by sa zvážiť možnosť neuložiť povinnosť uchovávať údaje všetkým poskytovateľom elektronických komunikačných služieb, ale uložiť túto povinnosť v závislosti od ich veľkosti a druhu služieb, ktoré ponúkajú, pričom by došlo napríklad k vylúčeniu tých, ktorí ponúkajú vysokošpecializované služby.

75 Povoľovacie systémy by mohli byť založené na pravidelnom vyhodnocovaní hrozieb v každom členskom štáte. Je potrebné zaručiť, aby vznikla súvislosť medzi uchovávanými údajmi a sledovaným cieľom a aby táto súvislosť zodpovedala konkrétnej situácii v každom členskom štáte. Preto by povolenia na uchovávanie udelené poskytovateľom mohli viesť k uchovávaniu určitých typov údajov počas určitého obdobia v závislosti od vyhodnotenia hrozby. Tieto povolenia by mohol udeľovať súd alebo nezávislý správny orgán a pravidelne by sa skúmalo, či je toto uchovávanie nevyhnutné.

94. V praxi to znamená, že – pokiaľ ide o dve hlavné kategórie (údaje o prenose dát a údaje o polohe) – treba na základe vhodných kritérií uchovávať len *minimum* údajov, ktoré sa považujú za úplne nevyhnutné pre účinné predchádzanie a potláčanie trestnej činnosti a pre ochranu národnej bezpečnosti.

95. Prináleží členským štátom alebo inštitúciám Únie vykonať túto voľbu prostredníctvom právnych predpisov (s pomocou svojich expertov), pričom musia upustiť od akéhokoľvek pokusu vyžadovať všeobecné a nediferencované uchovávanie všetkých údajov o prenose dát a polohe.

96. Okrem toho obmedzenia podľa kategórií sa uchovávané údaje môžu uchovávať len počas určitej doby uchovávania, aby neumožnili zadovážiť si podrobný obraz o živote dotknutých osôb. Táto doba uchovávania sa musí navyše upraviť podľa povahy údajov, aby sa údaje, ktoré poskytujú presnejšie informácie o životnom štýle a zvyklostiach týchto osôb, uchovávali počas kratšieho časového obdobia.[76]

97. Inak povedané, jedným z prostriedkov, ktoré treba preskúmať, je odlíšenie doby uchovávania každej kategórie údajov v závislosti od ich užitočnosti pre dosiahnutie bezpečnostných cieľov. Obmedzením doby, počas ktorej sa súčasne uchovávajú jednotlivé kategórie údajov (a preto ich možno použiť na nájdenie súvislostí, ktoré svedčia o životnom štýle dotknutých osôb), sa rozširuje ochrana práva, ktoré zaručuje článok 8 Charty.

98. V tomto zmysle sa na pojednávaní vyjadril Európsky dozorný úradník ochrany údajov: čím viac bude kategórií uchovávaných metaúdajov a čím dlhšia bude doba uchovávania, tým ľahšie sa bude dať stanoviť podrobný profil osoby a naopak.[77]

99. Okrem toho, ako tiež bolo uvedené na pojednávaní, je zložité vymedziť hranicu medzi určitými metaúdajmi elektronických komunikácií a obsahom týchto komunikácií. Niektoré metaúdaje môžu mať rovnakú alebo väčšiu výpovednú hodnotu než samotný obsah týchto komunikácií: tak to môže byť v prípade adries (URL) navštívených webových stránok.[78] Preto by sa mala tomuto typu údajov a iným podobným údajom venovať osobitná pozornosť s cieľom čo najviac obmedziť potrebu a dobu ich uchovávania.

100. Nie je ľahké nájsť vyvážené riešenie, keďže postup spočívajúci v krížovom porovnávaní a párovaní uchovávaných údajov umožňuje vyšetrovacím a spravodajským službám identifikovať podozrivého, prípadne hrozbu. Napriek tomu sa uchovávanie údajov na odhalenie tohto podozrivého alebo tejto hrozby a uchovávanie údajov, ktorého výsledkom je podrobný obraz o živote osoby, líšia svojou intenzitou.

101. Kým sa neprijmú spoločné pravidlá pre celú Úniu v tejto konkrétnej oblasti, podľa môjho názoru nemožno žiadať Súdny dvor, aby na seba vzal regulačné úlohy a podrobne spresnil, ktoré kategórie údajov možno uchovávať a na akú dobu ich možno uchovávať. Prislúcha inštitúciám

[76] Taký systém sa podľa všetkého uplatňuje v Spolkovej republike Nemecko, ktorej vláda na pojednávaní uviedla, že podľa jej právnych predpisov je doba uchovávania údajov o prenose dát desať týždňov, zatiaľ čo doba uchovávania údajov o polohe je len štyri týždne. Naopak podľa Francúzskej republiky je nevyhnutná ročná doba uchovávania údajov o prenose dát a polohe. Podľa tohto členského štátu skrátenie tejto doby na menej ako jeden rok by malo za následok zníženie efektivity činnosti justičnej polície.

[77] Samozrejme, treba zaručiť, aby poskytovatelia elektronických komunikačných služieb po uplynutí doby uchovávania natrvalo zmazali údaje (s výnimkou údajov, ktoré môžu naďalej uchovávať na obchodné účely v súlade so smernicou 2002/58).

[78] Na pojednávaní francúzska vláda uviedla, že URL sú vyňaté z údajov o pripojení, pre ktoré jej právne predpisy stanovujú všeobecnú povinnosť uchovávania.

Únie a členským štátom, aby po určení hraníc, ktoré podľa Súdneho dvora vyplývajú z Charty, našli správny spôsob na dosiahnutie rovnováhy medzi ochranou bezpečnosti a základných práv chránených Chartou.

102. Je pravda, že ak by neboli k dispozícii informácie, ktoré možno vyvodiť z väčšieho počtu uchovávaných údajov, mohlo by to v niektorých prípadoch sťažiť boj proti potenciálnym hrozbám. To je však jedna z daní, ktoré musia orgány verejnej moci zaplatiť, ak si samy uložia povinnosť chrániť základné práva.

103. Tak ako by nikto nepodporil povinnosť *ex ante* spočívajúcu vo všeobecnom a nediferencovanom uchovávaní *obsahu* súkromných elektronických komunikácií (a to ani v prípade, ak by právne predpisy zaručovali obmedzený neskorší prístup k tomuto obsahu), ani metaúdaje týchto komunikácií, ktoré môžu vyjadrovať také citlivé informácie ako samotný obsah, sa nemajú uchovávať nediferencovane a všeobecne.

104. Legislatívne ťažkosti – ktoré uznávam – spojené s presným vymedzením prípadov a podmienok, za ktorých možno vykonávať cielené uchovávanie, neodôvodňujú, aby členské štáty urobili z výnimky pravidlo a zmenili všeobecné uchovávanie osobných údajov na základnú zásadu svojich právnych predpisov. Ak by to bolo tak, pripustila by sa časovo neobmedzená platnosť významného zásahu do práva na ochranu osobných údajov.

105. Musím dodať, že nič nebráni tomu, aby v naozaj *výnimočných* situáciách, ktoré sa vyznačujú bezprostrednou hrozbou alebo mimoriadnym nebezpečenstvom a 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.

106. Za týchto okolností by bolo možné prijať právnu úpravu, ktorá konkrétne povolí širšie uchovávanie údajov (a prístup k nim) podľa podmienok a postupov, ktoré zabezpečia, že tieto opatrenia budú mať výnimočný charakter, pokiaľ ide o ich vecný dosah a časovú pôsobnosť, ako aj príslušné súdne záruky.

107. Z porovnávacieho preskúmania normatívnych režimov, ktoré upravujú krízové ústavné situácie, vyplýva, že nie je nemožné vymedziť prípady, ktoré môžu viesť k uplatneniu osobitného normatívneho režimu, a stanoviť, ktorý orgán môže prijať toto rozhodnutie, za akých podmienok a pod akým dohľadom.[79]

E. Konkrétne odpovede na tri prejudiciálne otázky

1. Úvodná úvaha

108. Vnútroštátny súd žiada o výklad článku 15 ods. 1 smernice 2002/58 v spojení s viacerými právami zaručenými Chartou, ktorými sú: právo na rešpektovanie súkromného a rodinného života (článok 7), právo na ochranu osobných údajov (článok 8) a právo na slobodu prejavu a na informácie (článok 11).

[79] ACKERMAN, B.: The Emergency Constitution. In: *Yale Law Journal*, zv. 113, 2004, s. 1029 až 1092; FEREJOHN, J., PASQUINO, S.: The Law of the Exception: A Typology of Emergency Powers. In: *International Journal of Constitutional Law*, zv. 2, 2004, s. 210 až 239.

109. Ako vysvetľujem v návrhoch vo veciach C-511/18 a C-512/18, práve uvedené práva by totiž podľa Súdneho dvora mohli byť v týchto prípadoch dotknuté.

110. Cour constitutionnelle (Ústavný súd) však poukazuje aj na články 4 a 6 Charty, ktorých sa týka druhá, resp. prvá prejudiciálna otázka.

111. Pokiaľ ide o článok 6 Charty, ktorý zaručuje právo na slobodu a bezpečnosť, tento článok bol uvedený aj vo veciach C-511/18 a C-512/18 a k jeho relevantnosti som sa vyjadril v príslušných návrhoch, na ktoré odkazujem.[80]

112. Čo sa týka článku 4 Charty, keďže odpoveď nezávisí od rozboru vnútroštátnych právnych predpisov na účely ich porovnania s právom Únie, ale skôr od výkladu tohto ustanovenia, považujem za vhodné odpovedať najprv na túto otázku.

2. Druhá prejudiciálna otázka

113. Len v tomto prejudiciálnom konaní bol totiž uvedený odkaz na zákaz mučenia a neľudského alebo ponižujúceho zaobchádzania alebo trestu, zaručený článkom 4 Charty, a preto mu musím venovať pozornosť.

114. Vnútroštátny súd chce odkazom na článok 4 Charty vyjadriť, že cieľom vnútroštátneho predpisu je tiež splniť *pozitívny záväzok* verejnej moci spočívajúci vo vytvorení „právneho rámca, ktorý umožní účinné vyšetrovanie a účinné potláčanie sexuálneho zneužívania maloletých osôb a tiež umožní skutočne identifikovať páchateľa trestného činu, a to aj vtedy, ak sa využívajú prostriedky elektronickej komunikácie“.[81]

115. Zastávam názor, že tento konkrétny *pozitívny záväzok* sa veľmi nelíši od každej z osobitných povinností, ktoré štátu vyplývajú z proklamácie katalógu základných práv. Právo na život (článok 2 Charty), právo na nedotknuteľnosť osoby (článok 3 Charty) alebo právo na ochranu osobných údajov (článok 8 Charty) – tak ako sloboda prejavu (článok 11 Charty) alebo sloboda myslenia, svedomia a náboženského vyznania (článok 10 Charty) – znamenajú pre štát povinnosť vytvoriť normatívny rámec, v ktorom bude zaručený ich účinný výkon, v prípade potreby prostredníctvom uplatnenia donucovacej moci orgánmi verejnej moci voči komukoľvek, kto chce zabrániť výkonu týchto práv alebo sťažiť ho.[82]

116. Pokiaľ ide o sexuálne zneužívanie maloletých osôb, ESĽP zastáva názor, že deti a iné zraniteľné osoby majú kvalifikované právo na štátnu ochranu prostredníctvom prijatia trestnoprávnych predpisov, ktoré účinne a s odstrašujúcimi účinkami sankcionujú páchanie týchto trestných činov.[83]

80 Návrhy vo veciach C-511/18 a C-512/18, bod 95 a nasl.

81 Znenie druhej otázky *in fine*. Tento odkaz na prostriedky elektronickej komunikácie vysvetľuje, prečo sa v tejto otázke spomína druhý *pozitívny záväzok* členských štátov, ktorý im vyplýva z článku 8 Charty v súvislosti s ochranou osobných údajov. Tento dvojnásobný odkaz na článok 8 Charty svedčí o tom, že vnútroštátny súd pripisuje právam zakotveným v Charte v závislosti od ich povahy dvojakú funkciu: funkciu spočívajúcu v *obmedzení* sporného záväzku a funkciu spočívajúcu v *odôvodnení* tohto záväzku.

82 Táto povinnosť týkajúca sa účinnosti sa mení na povinnosť verejnej moci dosiahnuť výsledok v sociálnom štáte alebo štáte poskytujúcom dávky, v ktorom je okrem formálneho priznania práv dôležité aj praktické uskutočnenie ich materiálneho obsahu.

83 Rozsudok ESĽP z 2. decembra 2008, K. U. v. Fínsko (ECHR:2008:1202JUD000287202, § 46).

117. Uvedené kvalifikované právo na ochranu nemá oporu len v článku 4 Charty, lebo sa prirodzene možno odvolávať aj na článok 1 (ľudská dôstojnosť) alebo článok 3 (právo na telesnú a duševnú nedotknuteľnosť).

118. Hoci pri posudzovaní právnych záujmov, ktorých sa dotýka vnútroštátna právna úprava [84], nemožno prehliadnuť pozitívny záväzok verejnej moci zaručiť ochranu deťom a iným zraniteľným osobám, tento záväzok sa tiež nemôže zmeniť na „neprimeranú záťaž“ pre verejnú moc [85], ani sa nemôže plniť v rozpore so zákonom alebo bez rešpektovania ostatných základných práv [86].

3. Prvá prejudiciálna otázka

119. Vnútroštátny súd chce v podstate vedieť, či právo Únie bráni vnútroštátnemu zákonu, o ktorom má rozhodnúť v rámci návrhu na vyhlásenie predpisu za protiústavný.

120. Keďže Súdny dvor už podal výklad smernice 2002/58, ktorý je v súlade s príslušnými ustanoveniami Charty, pri zodpovedaní prejudiciálnej otázky treba vziať do úvahy judikatúru sformulovanú v rozsudku Tele2 Sverige a Watson, prípadne s úpravami, ktoré sa doplnia teraz.

121. Vychádzajúc z uvedeného predpokladu, výkladové usmernenia, ktoré možno poskytnúť pre Cour constitutionnelle (Ústavný súd), aby sám posúdil súlad vnútroštátneho predpisu s právom Únie, sa musia samostatne týkať uchovávania a prístupu k údajom, ako sú upravené v tomto vnútroštátnom predpise.

a) Podmienky uchovávania údajov

122. Belgická vláda zdôrazňuje, že chcela vytvoriť jasný právny rámec, ktorý by zahŕňal záruky potrebné na ochranu súkromného života, namiesto toho, aby sa opierala o prax prevádzkovateľov elektronických komunikačných služieb týkajúcu sa uchovávania údajov na účely fakturácie a spracúvania žiadostí klientov o informácie.

123. Uvedená vláda sa domnieva, že účelom všeobecnej a preventívnej povinnosti uchovávať údaje nie je len pátranie, vyšetrovanie a stíhanie závažných trestných činov, ale aj zaručenie národnej bezpečnosti, obrany územia a verejnej bezpečnosti, vyšetrovanie, odhaľovanie a stíhanie menej závažných trestných činov alebo zabránenie nepovolenému používaniu systémov elektronickej komunikácie [87] alebo ktorýkoľvek iný cieľ uvedený v článku 23 ods. 1 nariadenia 2016/679.

84 V tejto súvislosti sa domnievam, že k právam, ktoré uvádza vnútroštátny súd (ako *obmedzenia* sporného záväzku, a nie ako jeho *odôvodnenie*), by sa mohlo doplniť právo na účinný prostriedok nápravy (článok 47 Charty) alebo právo na obhajobu (článok 48 Charty), ktorých prípadné porušenie tiež bolo predmetom diskusie v konaniach vo veci samej. Vo výroku návrhu na začatie prejudiciálneho konania sú však spomenuté len články 7, 8 a 11 a článok 52 ods. 1 Charty.

85 Rozsudok ESĽP z 28. októbra 1998, Osman v. Spojené kráľovstvo (CE:ECHR:1998:1028JUD002345294, § 116).

86 Tamže, § 116 in fine: „[je potrebné] zabezpečiť, aby polícia vykonávala svoju právomoc týkajúcu sa boja proti trestnej činnosti a predchádzania trestnej činnosti v úplnom súlade so zákonnými postupmi a ostatnými zárukami, ktoré legitímne obmedzujú rozsah jej vyšetrovacích úkonov v trestnom konaní“. Pozri tiež rozsudok ESĽP z 2. decembra 2008, K. U. v. Fínsko (CE:ECHR:2008:1202JUD000287202, § 48). Súdny dvor v tom istom zmysle v rozsudku z 29. júla 2019, Gambino a Hyka (C-38/18, EU:C:2019:628, bod 49), rozhodol, že práva priznané obeti trestného činu nemôžu mať vplyv na skutočné uplatňovanie práv priznaných obvinenej osobe.

87 Táto povinnosť je odôvodnená aj na účely odpovede na hovor tiesňovej službe alebo vypátrania nezvestnej osoby, ktorej telesná integrita je bezprostredne ohrozená.

124. Podľa belgickej vlády:

– uchovávanie údajov ako také neumožňuje vyvodiť veľmi presné závery o súkromnom živote dotknutých osôb: možnosť vyvodiť také závery by vznikla len v rozsahu, v akom by sa tiež poskytol prístup k uchovávaným údajom;

– zákon obsahuje záruky určené na ochranu súkromia; okrem iného sa uchovávanie údajov nedotýka obsahu komunikácie; v plnom rozsahu sa uplatňujú záruky, pokiaľ ide o odôvodnenie uchovávania, právo na prístup, právo na opravu a iné práva; poskytovatelia a operátori musia uplatňovať na uchovávané údaje tie isté povinnosti a opatrenia týkajúce sa bezpečnosti a ochrany, aké sa vzťahujú na údaje v sieti, pričom ich musia chrániť pred náhodným alebo nezákonným zničením, náhodnou stratou alebo zmenou;

– údaje sa môžu uchovávať 12 mesiacov (po uplynutí tejto doby sa musia zničiť), a to len na území Únie;

– poskytovatelia a operátori musia uplatňovať opatrenia technickej ochrany, ktoré zabezpečia, že uchovávané údaje sa od okamihu ich zaznamenania stanú nečitateľnými a nepoužiteľnými pre akúkoľvek osobu, ktorá nemá povolený prístup k takýmto údajom;

– tieto operácie sa v každom prípade vykonávajú pod dohľadom belgického regulačného orgánu pre odvetvia pôšt a telekomunikácií a orgánu pre ochranu osobných údajov.

125. Napriek týmto zárukám je nesporné, že belgické právne predpisy ukladajú operátorom a poskytovateľom elektronických komunikačných služieb všeobecnú a nediferencovanú povinnosť uchovávať údaje o prenose dát a polohe v zmysle smernice 2002/58 spracovávané v súvislosti s poskytovaním týchto služieb. Ako už bolo uvedené, doba uchovávania je vo všeobecnosti 12 mesiacov: nie je stanovené nijaké časové obmedzenie v závislosti od kategórií uchovávaných údajov.

126. Uvedená všeobecná a nediferencovaná povinnosť uchovávania platí trvalo a sústavne. Aj keď je jej cieľom prevencia, vyšetrovanie a stíhanie všetkých trestných činov (od trestných činov súvisiacich s národnou bezpečnosťou alebo obranou alebo obzvlášť závažných trestných činov až po trestné činy, za ktoré možno uložiť trest odňatia slobody v trvaní kratšom ako jeden rok), takáto povinnosť nie je v súlade s judikatúrou Súdneho dvora, takže ju nemožno považovať za zlučiteľnú s Chartou.

127. Na dosiahnutie súladu s uvedenou judikatúrou bude musieť belgický zákonodarca preskúmať iné prostriedky (ako sú napríklad prostriedky, ktoré som spomenul vyššie) na zavedenie vzorcov obmedzeného uchovávania. Tieto vzorce, ktoré sa budú meniť v závislosti od kategórií údajov, musia zodpovedať zásade, že sa má uchovávať len *minimum* údajov, ktoré je nevyhnutné v závislosti od nebezpečenstva a hrozby, a to na obmedzenú dobu, ktorá závisí od povahy uchovávaných informácií. Uchovávanie v každom prípade nemôže poskytovať presný *harmonogram* súkromného života, zvyklostí, správania alebo spoločenských vzťahov dotknutých osôb.

b) Podmienky prístupu orgánov verejnej moci k uchovávaným údajom

128. Domnievam sa, že podmienky uvedené v rozsudku Tele2 Sverige a Watson [88] sú naďalej relevantné, aj pokiaľ ide o prístup: vnútroštátna právna úprava musí stanoviť hmotnoprávne a procesnoprávne podmienky prístupu príslušných orgánov k uchovávaným údajom [89].

129. Belgická vláda spresňuje, že článok 126 ods. 2 zákona z roku 2005 (o elektronických komunikáciách) [90] reštriktívne vymedzuje vnútroštátne orgány, ktoré môžu získať údaje uchovávané v súlade s odsekom 1 tohto článku.

130. Medzi uvedenými orgánmi sa nachádzajú súdne orgány a prokuratúra, štátne bezpečnostné zložky, Generálna spravodajská a bezpečnostná služba pod kontrolou jednotlivých nezávislých komisií, príslušníci justičnej polície Belgického inštitútu pre poštové služby a telekomunikácie, tiesňové služby, príslušníci justičnej polície Jednotky nezvestných osôb Federálnej polície, Mediačná služba pre oblasť telekomunikácií a úrad pre dohľad nad finančným sektorom.

131. Belgická vláda všeobecne tvrdí, že vnútroštátne právne predpisy nedovoľujú, aby jednotlivé služby získali prístup k údajom na účely aktívneho stíhania neidentifikovaných hrozieb alebo hrozieb bez konkrétnych indícií. Vnútroštátne orgány teda nemôžu priamo získať prístup k nefiltrovaným komunikačným údajom a automaticky ich spracovať s cieľom získať informácie a aktívne predchádzať bezpečnostným rizikám.

132. Podľa uvedenej vlády prístup k údajom podlieha prísnym podmienkam v závislosti od postavenia každého z príslušných vnútroštátnych orgánov.

133. Na zodpovedanie prvej prejudiciálnej otázky podľa môjho názoru nie je potrebné, aby Súdny dvor vykonal komplexnú analýzu podmienok, ktoré musí splniť každý z týchto orgánov, aby mohol získať uchovávané údaje. Uvedená úloha prináleží skôr vnútroštátnemu súdu, ktorý ju bude musieť splniť so zreteľom na usmernenia vyplývajúce z rozsudkov Tele2 Sverige a Watson a Ministerio Fiscal.

134. Okrem toho podľa informácií, ktoré poskytla belgická vláda, existujú značné rozdiely medzi podmienkami prístupu, ktoré sa týkajú súdnych orgánov alebo prokuratúry [91] na účely pátrania, vyšetrovania a stíhania trestných činov v zmysle článkov 46a [92] a 88a [93] Trestného poriadku, a podmienkami, ktoré platia pre iné orgány.

88 Pozri bod 60 týchto návrhov.

89 Rozsudok Tele2 Sverige a Watson, bod 118.

90 Článok 126 v znení zákona z 29. mája 2016.

91 Otázka, či prokuratúra môže vydávať také opatrenia, je predmetom prebiehajúceho prejudiciálneho konania vo veci C-746/18, HK/Prokuratur.

92 Na vyžiadanie identifikačných údajov od operátorov je príslušná prokuratúra, ktorá ich vyžiada odôvodneným písomným (v naliehavých prípadoch ústnym) rozhodnutím, v ktorom sa preukáže primeranosť opatrenia s ohľadom na rešpektovanie súkromného života a jeho subsidiárny charakter vo vzťahu k akejkoľvek inej vyšetrovacej povinnosti. V prípade trestných činov, za ktoré nemožno uložiť hlavný trest odňatia slobody v trvaní jedného roka alebo prísnejší trest, prokurátor môže požiadať o údaje len za šesť mesiacov pred vydaním svojho rozhodnutia.

93 Na vyžiadanie presnej polohy elektronickej komunikácie alebo uchovávaných údajov o prenose dát a polohe od operátorov je príslušný sudca pre prípravné konanie, ktorý môže prijať toto opatrenie, ak existujú vážne dôvody, na základe ktorých sa možno domnievať, že došlo k spáchaniu trestného činu, za ktorý možno uložiť určitý trest, odôvodneným písomným (v naliehavých prípadoch ústnym) uznesením, pričom sa uplatnia tie isté požiadavky primeranosti a subsidiarity, ktoré platia pre prokuratúru. Existujú určité výnimky, ak predmetné opatrenie smeruje proti určitým chráneným profesijným kategóriám (ako sú napríklad advokáti alebo lekári).

135. Čo sa týka spravodajských a bezpečnostných služieb, podľa zákona z roku 1998 musí byť žiadosť o sprístupnenie údajov o prenose dát a polohe, ktoré majú k dispozícii operátori, založená na objektívnych kritériách s cieľom zaručiť, aby bola obmedzená na to, čo je prísne nevyhnutné, na základe vopred identifikovanej hrozby.[94] Sú stanovené rôzne lehoty prístupu (šesť, deväť alebo dvanásť mesiacov) v závislosti od potenciálnej hrozby, pričom žiadosť musí byť v súlade so zásadami proporcionality a subsidiarity. Bol tiež zavedený kontrolný mechanizmus, za ktorý zodpovedá nezávislý orgán.[95]

136. Pokiaľ ide o príslušníkov justičnej polície Belgického inštitútu pre poštové služby a telekomunikácie (Belgisch Instituut voor postdiensten en telecommunicatie – BIPT), tieto osoby môžu získať prístup k údajom, ktorými disponujú telekomunikační operátori, pod dohľadom prokuratúry vo veľmi obmedzených konkrétnych prípadoch[96], pričom ich činnosť sa podľa belgickej vlády nedotýka osôb, ktorých údaje sa uchovávajú.

137. Čo sa týka tiesňových služieb, ktoré poskytujú pomoc na mieste, tieto služby môžu požiadať o údaje volajúceho, ktorý uskutočnil tiesňový hovor, ak po uskutočnení tohto hovoru nezískajú od poskytovateľa alebo operátora identifikačné údaje tohto volajúceho alebo ak sú tieto údaje neúplné alebo nesprávne.

138. Pokiaľ ide o príslušníkov justičnej polície Jednotky nezvestných osôb Federálnej polície, títo príslušníci si môžu vyžiadať od operátora údaje potrebné na vypátranie nezvestnej osoby, ktorej telesná integrita je bezprostredne ohrozená. Prístup, ktorý podlieha prísnym podmienkam, je obmedzený na údaje umožňujúce identifikáciu užívateľa a údaje o prístupe a pripojení koncového zariadenia k sieti a k službe, ako aj údaje o polohe tohto zariadenia a vzťahuje sa len na údaje uchovávané počas 48 hodín pred podaním žiadosti.

139. Čo sa týka Mediačnej služby pre oblasť telekomunikácií, tento orgán si môže vyžiadať len identifikačné údaje osoby, ktorá zneužila sieť alebo službu elektronickej komunikácie. V tomto prípade nedochádza k predchádzajúcemu preskúmaniu zo strany súdu alebo nezávislého správneho orgánu (iného, než je uvedená služba).

140. Napokon úrad pre dohľad nad finančným sektorom môže na účely boja proti finančnej trestnej činnosti s predchádzajúcim povolením sudcu pre prípravné konanie získať prístup k údajom o prenose dát a polohe.

141. Opis týchto pravidiel a podmienok prístupu k uchovávaným údajom, ktoré platia pre každý z orgánov oprávnených získať ich, svedčí o rozličných prípadoch a zárukách, ktorých súlad s kritériami, ktoré vo svojej judikatúre používa Súdny dvor[97], musí podrobne preskúmať vnútroštátny súd.

94 V rozhodnutí sa podľa konkrétneho prípadu uvedú fyzické alebo právnické osoby, združenia alebo skupiny, veci, miesta, udalosti alebo informácie, na ktoré sa vzťahuje osobitná metóda. Musí v ňom byť uvedená aj súvislosť medzi účelom vyžiadaných údajov a potenciálnou hrozbou, ktorá odôvodňuje túto konkrétnu metódu.

95 Správna komisia pre dohľad nad osobitnými a výnimočnými metódami zberu údajov spravodajskými a bezpečnostnými službami (komisia BIM) a Stály výbor pre kontrolu spravodajských služieb (výbor R). Belgická vláda uvádza, že komisia BIM je zodpovedná za monitorovanie pátracích metód používaných spravodajskými a bezpečnostnými službami, ktoré primárne kontroluje. Táto komisia, zložená zo sudcov, plní svoje úlohy úplne nezávisle. Je upravená aj sekundárna nezávislá kontrola, ktorú vykonáva výbor R.

96 Tento prístup je možný na účely vyšetrovania, pátrania a stíhania trestných činov uvedených v článku 114 (bezpečnosť sietí), článku 124 (dôvernosť elektronickej komunikácie) a článku 126 (uchovávanie údajov a prístup) zákona z 13. júna 2005 o elektronických komunikáciách.

97 Odkazujem na bod 60 týchto návrhov

142. Poukazujem napríklad na to, že v kontexte sporných právnych predpisov príslušné vnútroštátne orgány zrejme nemajú povinnosť informovať dotknuté osoby (pokiaľ táto informácia neohrozí prebiehajúce vyšetrovanie) o tom, že došlo k poskytnutiu ich údajov. Tiež sa nezdá, že sú stanovené – aspoň v niektorých prípadoch, ako sú prípady týkajúce sa finančných trestných činov – vopred určené pravidlá týkajúce sa závažnosti týchto trestných činov na odôvodnenie prístupu k príslušným údajom. Súvislosť medzi intenzitou zásahu a závažnosťou prešetrovaného trestného činu v zmysle rozsudku Ministerio Fiscal nie je vo všetkých prípadoch zrejmá.

143. V každom prípade sa domnievam, že úvahy súvisiace s prístupom orgánov k údajom sú druhoradé, ak je – z dôvodov, ktoré som už uviedol – hlavným dôvodom, pre ktorý vnútroštátne právne predpisy, ktorých sa týka toto prejudiciálne konanie, nie sú v súlade s právom Únie, samotné všeobecné a nediferencované uchovávanie týchto údajov.

4. Tretia prejudiciálna otázka

144. Cour constitutionnelle (Ústavný súd) sa pýta, či v prípade, ak by sa vzhľadom na odpoveď Súdneho dvora rozhodlo, že vnútroštátne právne predpisy sú nezlučiteľné s právom Únie, by mohol dočasne zachovať účinky týchto právnych predpisov. Zabránilo by sa tak právnej neistote a umožnilo by sa, aby sa zhromažďované a uchovávané údaje mohli naďalej používať na dosahovanie sledovaných cieľov.

145. Z ustálenej judikatúry vyplýva, že „jedine Súdny dvor môže výnimočne a z naliehavých dôvodov právnej istoty priznať dočasné pozastavenie účinku neuplatnenia, ktorý spôsobuje právne pravidlo Únie voči vnútroštátnemu právu, ktoré je v rozpore s týmto pravidlom“. Ak by „mali vnútroštátne súdy právomoc priznať vnútroštátnym ustanoveniam prednosť pred ustanoveniami práva Únie, s ktorými sú v rozpore, hoci len dočasne, bolo by narušené jednotné uplatňovanie práva Únie“. [98]

146. Komisia sa domnieva, že vzhľadom na to, že Súdny dvor neobmedzil časové účinky výkladu článku 15 ods. 1 smernice 2002/58, na túto otázku vnútroštátneho súdu treba odpovedať záporne. [99]

147. Súdny dvor však v rozsudku z 28. februára 2012, Inter-Environnement Wallonie a Terre wallonne [100], konštatoval, že vzhľadom na existenciu naliehavého záujmu na ochrane životného prostredia mohlo byť vnútroštátnemu súdu výnimočne povolené, aby uplatnil vnútroštátne ustanovenie, ktoré ho oprávňovalo zachovať určité účinky vnútroštátneho aktu, ktorý bol zrušený v dôsledku porušenia predpisu Únie. [101]

98 Rozsudok z 28. júla 2016, Association France Nature Environnement (C-379/15, EU:C:2016:603, bod 33).

99 Bod 100 písomných pripomienok Komisie.

100 Vec C-41/11, EU:C:2012:103.

101 Rozsudok z 28. februára 2012, Inter-Environnement Wallonie a Terre wallonne (C-41/11, EU:C:2012:103, bod 58). Súdny dvor v rozsudku z 28. júla 2016, Association France Nature Environnement (C-379/15, EU:C:2016:603, bod 34), z uvedeného konštatovania vyvodil, že „priznáva vnútroštátnemu súdu v jednotlivých prípadoch a výnimočne možnosť upraviť účinky zrušenia vnútroštátneho ustanovenia, v prípade ktorého bolo rozhodnuté, že je nezlučiteľné s právom Únie“.

148. Táto judikatúra bola potvrdená rozsudkom z 29. júla 2019, Inter-Environnement Wallonie a Bond Beter Leefmilieu Vlaanderen [102]. Hoci tento rozsudok bol vydaný v oblasti ochrany životného prostredia, resp. založený na bezpečnosti zásobovania elektrickou energiou, nevidím dôvod, prečo by sa nemal uplatniť v iných oblastiach práva Únie, najmä v oblasti, o ktorú ide v prejednávanej veci.

149. Ak „naliehavý záujem na ochrane životného prostredia“ môže odôvodniť, aby vnútroštátne súdy výnimočne zachovali určité účinky vnútroštátneho ustanovenia nezlučiteľného s právom Únie, je to preto, lebo ochrana životného prostredia tvorí „jeden zo základných cieľov Európskej únie a má prierezový a fundamentálny charakter“. [103]

150. K cieľom Únie pritom patrí aj vytvorenie priestoru bezpečnosti (článok 3 ZEÚ), ktorý zahŕňa rešpektovanie základných štátnych funkcií, najmä udržiavanie verejného poriadku a zabezpečovanie národnej bezpečnosti (článok 4 ods. 2 ZEÚ). Tento cieľ je rovnako „prierezový a fundamentálny“ ako ochrana životného prostredia, lebo jeho dosiahnutie je nevyhnutnou podmienkou vytvorenia normatívneho rámca spôsobilého zaručiť účinný výkon základných práv a slobôd.

151. Podľa môjho názoru by naliehavé dôvody súvisiace s ochranou národnej bezpečnosti v tejto veci mohli odôvodniť, aby Súdny dvor výnimočne povolil vnútroštátnemu súdu zachovať aspoň niektoré z účinkov sporného zákona.

152. Predpokladom uvedeného zachovania by bolo, aby vnútroštátny súd vzhľadom na rozhodnutie Súdneho dvora označil vnútroštátny predpis za nezlučiteľný s právom Únie a považoval dôsledky pre verejnú bezpečnosť alebo bezpečnosť štátu, ktoré by mohli vyplynúť z bezprostredného zrušenia (ak by následkom uvedenej nezlučiteľnosti podľa vnútroštátneho práva bolo zrušenie) alebo neuplatňovania tohto predpisu, za mimoriadne škodlivé.

153. Dočasné zachovanie (všetkých alebo niektorých) účinkov vnútroštátneho predpisu by si navyše vyžadovalo, aby

– cieľom tohto zachovania bolo zabrániť právnemu vákuu týkajúcemu sa takých škodlivých účinkov, aké vyplývajú z uplatňovania spornej právnej úpravy, pričom tomuto vákuu nemožno zamedziť inými prostriedkami a jeho dôsledkom by bolo, že vnútroštátne orgány by prišli o dôležitý nástroj na zaručenie bezpečnosti štátu, a

– trvalo len nevyhnutný čas potrebný na prijatie opatrení umožňujúcich nápravu zistenej nezlučiteľnosti s právom Únie. [104]

154. V prospech tohto riešenia svedčia navyše ťažkosti, ktoré vyvoláva zosúladenie vnútroštátnych právnych úprav s judikatúrou sformulovanou vo veci Tele2 Sverige a Watson [105], a skutočnosť, že belgický zákonodarca vyjadril svoju vôľu tým, že vyhovel rozsudku Digital Rights a zmenil svoje právne predpisy. Táto skutočnosť vzbudzuje dojem, že tiež zosúladí zákon z 29. mája 2016 (prijatý pred tým, ako bol známy rozsudok Tele2 Sverige a Watson) s judikatúrou sformulovanou v tomto poslednom uvedenom rozsudku.

102 Vec C-411/17, EU:C:2019:622, bod 178.

103 Rozsudok z 28. februára 2012, Inter-Environnement Wallonie a Terre wallonne (C-41/11, EU:C:2012:103, bod 57).

104 Rozsudok z 28. februára 2012, Inter-Environnement Wallonie a Terre wallonne (C-41/11; EU:C:2012:103, bod 62).

105 Bod 45 písomných pripomienok dánskej vlády.

V. Návrh

155. Na základe vyššie uvedeného navrhujem, aby Súdny dvor odpovedal na prejudiciálne otázky, ktoré mu položil Cour constitutionnelle (Ústavný súd, Belgicko), takto:

1. 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

   – bráni vnútroštátnej právnej úprave, ktorá ukladá operátorom a poskytovateľom elektronických komunikačných služieb povinnosť všeobecne a nediferencovane uchovávať údaje o prenose dát a polohe všetkých účastníkov a užívateľov v súvislosti so všetkými prostriedkami elektronickej komunikácie;

   – na tomto závere nič nemení skutočnosť, že cieľmi uvedenej vnútroštátnej právnej úpravy nie sú len vyšetrovanie, odhaľovanie a stíhanie trestných činov bez ohľadu na to, či sú závažné, ale aj národná bezpečnosť, obrana územia, verejná bezpečnosť, zabránenie nepovolenému používaniu elektronických komunikačných systémov alebo ktorýkoľvek iný cieľ uvedený v článku 23 ods. 1 nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov);

   – na tomto závere nič nemení ani skutočnosť, že prístup k uchovávaným údajom podlieha podrobne upraveným zárukám. Je úlohou vnútroštátneho súdu overiť, či vnútroštátna právna úprava, ktorá upravuje podmienky prístupu príslušných orgánov k týmto údajom, obmedzuje tento prístup na osobitné prípady, ktorých závažnosť si nevyhnutne vyžaduje predmetný zásah, či ho podmieňuje predchádzajúcim preskúmaním (okrem naliehavých prípadov) zo strany súdu alebo nezávislého správneho orgánu a či stanovuje, aby dotknuté osoby boli informované o prístupe k týmto údajom, pokiaľ toto oznámenie neohrozí postup uvedených orgánov.

2. Články 4 a 6 Charty základných práv Európskej únie nemajú vplyv na výklad článku 15 ods. 1 smernice 2002/58 v spojení s ostatnými vyššie uvedenými článkami tejto Charty v tom zmysle, že by bránili konštatovaniu nezlučiteľnosti vnútroštátnej právnej úpravy, o akú ide v konaní vo veci samej, s právom Únie.

3. Vnútroštátny súd môže – ak mu to vnútroštátne právo dovoľuje – výnimočne a dočasne zachovať účinky právnej úpravy, o akú ide v konaní vo veci samej, aj keby bola nezlučiteľná s právom Únie, ak je toto zachovanie odôvodnené naliehavými dôvodmi súvisiacimi s hrozbami pre verejnú bezpečnosť alebo národnú bezpečnosť, proti ktorým nemožno bojovať inými prostriedkami a inými alternatívnymi opatreniami. Toto zachovanie môže trvať len nevyhnutný čas potrebný na nápravu uvedenej nezlučiteľnosti s právom Únie.