SÚDNY DVOR
EURÓPSKEJ ÚNIE

SK

Tematický súhrn
Ochrana osobných údajov

Riaditeľstvo výskumu a dokumentácie

curia.europa.eu

Úvod

Právo na ochranu osobných údajov je základným právom, ktorého dodržiavanie predstavuje významný cieľ pre Európsku úniu.

Je zakotvené v primárnom práve, najmä v článku 8 Charty základných práv Európskej únie (ďalej len „Charta“), ako aj v článku 16 ods. 1 Zmluvy o fungovaní Európskej únie (ZFEÚ). Toto základné právo je okrem iného úzko spojené s právom na rešpektovanie súkromného a rodinného života, zakotveným v článku 7 Charty.

Pokiaľ ide o sekundárne právo, od druhej polovice 90. rokov prijalo Európske spoločenstvo rôzne nástroje, ktorých účelom je zabezpečovať ochranu osobných údajov. Smernica 95/46/ES o ochrane fyzických osôb pri spracovaní osobných údajov a voľnom pohybe týchto údajov[1], zrušená od roku 2018, predstavovala v tejto súvislosti základný právny akt Únie v danej oblasti.

Smernicu 95/46 následne doplnila smernica 2002/58/ES[2] tým, že harmonizovala právne predpisy členských štátov týkajúce sa ochrany práva na súkromný život, pokiaľ ide najmä o spracovanie osobných údajov v sektore elektronických komunikácií.[3] Treba poznamenať, že normotvorca Únie s cieľom zohľadniť nový vývoj technológií a trhu začal od roku 2017 s opätovným preskúmaním tejto smernice[4], ktoré stále prebieha[5].

V roku 2016 Európska únia zmenila v danej oblasti všeobecný právny rámec. Na tento účel prijala nariadenie (EÚ) 2016/679[6] o ochrane osobných údajov (ďalej len „GDPR“), ktorým sa zrušuje smernica 95/46 a ktoré je priamo uplatniteľné od 25. mája 2018, ako aj smernicu (EÚ) 2016/680[7] týkajúcu sa ochrany uvedených údajov v trestných veciach, ktorej ustanovenia sa uplatňujú od 6. mája 2018.

---

1 Smernica Európskeho parlamentu a Rady 95/46/EHS 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), konsolidované znenie z 20. novembra 2003, zrušená od 25. mája 2018 (pozri poznámku pod čiarou 6).

2 Smernica Európskeho parlamentu a Rady 2002/58/ES 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), konsolidované znenie z 19. decembra 2009.

3 Smernica 2002/58/ES bola zmenená smernicou Európskeho parlamentu a Rady 2006/24/ES z 15. marca 2006 o uchovávaní údajov vytvorených alebo spracovaných v súvislosti s poskytovaním verejne dostupných elektronických komunikačných služieb alebo verejných komunikačných sietí a o zmene a doplnení smernice 2002/58/ES (Ú. v. EÚ L 105, 2006, s. 54). Túto smernicu Súdny dvor vyhlásil za neplatnú v rozsudku z 8. apríla 2014, Digital Rights Ireland a Seitlinger a i. (C-293/12 a C-594/12, EU:C:2014:238), z dôvodu, že vážne zasahovala do práva na rešpektovanie súkromného života a do ochrany osobných údajov (pozri rubriku I.1. tohto súhrnu, nazvanú „Súlad sekundárneho práva Únie s právom na ochranu osobných údajov“).

4 Komisia 10. januára 2017 predložila návrh na nahradenie tejto smernice nariadením o súkromí a elektronických komunikáciách.

5 Rada Európskej únie 10. februára 2021 schválila mandát na rokovanie o preskúmaní pravidiel ochrany súkromia a dôvernosti pri používaní elektronických komunikačných služieb, čo umožnilo začať rokovania s Európskym parlamentom. Znenie návrhu o rešpektovaní súkromného života a ochrane osobných údajov v elektronických komunikáciách a o zrušení smernice 2002/58/ES (nariadenie „o súkromí a elektronických komunikáciách“) je dostupný na: *https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_6087_2021_INIT&from=EN*.

6 Nariadenie 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 (Ú. v. EÚ L 119, 2016, s. 1).

7 Smernica Európskeho parlamentu a Rady (EÚ) 2016/680 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov príslušnými orgánmi na účely predchádzania trestným činom, ich vyšetrovania, odhaľovania alebo stíhania alebo na účely výkonu trestných sankcií a o voľnom pohybe takýchto údajov a o zrušení rámcového rozhodnutia Rady 2008/977/SVV (Ú. v. EÚ L 119, 2016, s. 89).

Pokiaľ ide o spracúvanie osobných údajov inštitúciami a orgánmi EÚ, ich ochrana je od 11. decembra 2018 zabezpečená najmä prostredníctvom nariadenia (EÚ) 2018/1725[8]. V záujme koherentného prístupu k ochrane osobných údajov v celej Únii má toto nariadenie za cieľ v čo najväčšej možnej miere zjednotiť pravidlá v danej oblasti s režimom zavedeným GDPR.

Napokon s cieľom reagovať na výzvy, ktoré prinášajú nové technológie, normotvorca Únie inicioval od roku 2020 prijatie nových legislatívnych opatrení,[9] ktoré sú prepojené s ustanoveniami práva Únie týkajúcimi sa ochrany osobných údajov.

Vzhľadom na rozsiahlu judikatúru Súdneho dvora v oblasti ochrany osobných údajov je cieľom tohto tematického súhrnu predstaviť výber základných rozsudkov v tejto oblasti, ako aj rozsudkov, ktoré významne prispeli k rozvoju tejto judikatúry, s osobitným dôrazom na rozsudky vydané veľkou komorou Súdneho dvora. Konkrétnejšie má tento súhrn pokrývať tak judikatúru týkajúcu sa všeobecnej právnej úpravy v oblasti ochrany osobných údajov, ktorá vyplýva z výkladu smernice 95/46 a GDPR, ako aj judikatúru týkajúcu sa odvetvovej právnej úpravy, ktorá je zameraná najmä na odvetvie elektronických komunikácií a trestné právo. Okrem toho je jeho cieľom predstaviť výber rozsudkov týkajúcich sa právnych predpisov, ktoré sa uplatňujú prierezovo, pričom od začiatku zdôrazňuje rozhodujúcu úlohu Charty pri vývoji judikatúry.

---

8 Nariadenie Európskeho parlamentu a Rady (EÚ) 2018/1725 z 23. októbra 2018 o ochrane fyzických osôb pri spracúvaní osobných údajov inštitúciami, orgánmi, úradmi a agentúrami Únie a o voľnom pohybe takýchto údajov, ktorým sa zrušuje nariadenie (ES) č. 45/2001 a rozhodnutie č. 1247/2002/ES (Ú. v. EÚ L 295, 2018, s. 39).

9 V tejto súvislosti treba spomenúť najmä tri legislatívne iniciatívy: *i)* nariadenie Európskeho parlamentu a Rady (EÚ) 2022/868 z 30. mája 2022 o európskej správe údajov a o zmene nariadenia (EÚ) 2018/1724 (akt o správe údajov) (Ú. v. EÚ L 152, 2022, s. 1) a nariadenie Európskeho parlamentu a Rady (EÚ) 2023/2854 z 13. decembra 2023 o harmonizovaných pravidlách týkajúcich sa spravodlivého prístupu k údajom a ich používania, ktorým sa mení nariadenie (EÚ) 2017/2394 a smernica (EÚ) 2020/1828 (akt o údajoch) (Ú. v. EÚ L 2854, 2023, s. 1); *ii)* balík o digitálnych službách a trhoch, ktorý pozostáva z nariadenia Európskeho parlamentu a Rady (EÚ) 2022/2065 z 19. októbra 2022 o jednotnom trhu s digitálnymi službami a o zmene smernice 2000/31/ES (akt o digitálnych službách) (Ú. v. EÚ L 277, 2022, s. 1) a z nariadenia Európskeho parlamentu a Rady (EÚ) 2022/1925 zo 14. septembra 2022 o súťažeschopných a spravodlivých trhoch digitálneho sektora a o zmene smerníc (EÚ) 2019/1937 a (EÚ) 2020/1828 (akt o digitálnych trhoch) (Ú. v. EÚ L 265, 2022, s. 1); a *iii)* úplne prvý legislatívny návrh na vytvorenie regulačného rámca pre umelú inteligenciu, ktorý sa skonkretizoval prostredníctvom nariadenia o umelej inteligencii (*Ú. v. EÚ L 1689, 2024*).

Obsah

ÚVOD 3
I. PRÁVO NA OCHRANU OSOBNÝCH ÚDAJOV UZNANÉ CHARTOU ZÁKLADNÝCH PRÁV EURÓPSKEJ ÚNIE 6
1. Súlad sekundárneho práva Únie s právom na ochranu osobných údajov 6
2. Dodržiavanie práva na ochranu osobných údajov v rámci vykonávania práva Únie 17
II. SPRACOVANIE OSOBNÝCH ÚDAJOV V ZMYSLE VŠEOBECNEJ PRÁVNEJ ÚPRAVY V DANEJ OBLASTI 18
1. Pôsobnosť všeobecnej právnej úpravy 18
2. Pojem „osobné údaje“ 24
3. Pojem „spracovanie osobných údajov“ 26
4. Pojem „registračný systém osobných údajov“ 31
5. Pojem „prevádzkovateľ spracovania osobných údajov“ 31
6. Pojem „spoločný prevádzkovateľ“ 34
7. Podmienky zákonnosti spracovania osobných údajov 34
III. SPRACÚVANIE OSOBNÝCH ÚDAJOV V ZMYSLE ODVETVOVEJ PRÁVNEJ ÚPRAVY 40
1. Spracúvanie osobných údajov v sektore elektronických komunikácií 40
2. Spracúvanie osobných údajov v trestných veciach 58
IV. PRENOS OSOBNÝCH ÚDAJOV DO TRETÍCH KRAJÍN 62
V. OCHRANA OSOBNÝCH ÚDAJOV NA INTERNETE 70
1. Právo na vznesenie námietky proti spracovaniu osobných údajov („právo na zabudnutie“) 70
2. Spracovanie osobných údajov a práva duševného vlastníctva 71
3. Odstránenie odkazov na osobné údaje 73
4. Súhlas používateľa internetovej stránky s uchovávaním informácií 82
5. Spracúvanie osobných údajov na online sociálnych sieťach 84
VI. VNÚTROŠTÁTNE DOZORNÉ ORGÁNY 87
1. Rozsah požiadavky nezávislosti 87
2. Určenie uplatniteľného práva a príslušného dozorného orgánu 90
3. Právomoci vnútroštátnych dozorných orgánov 91
4. Podmienky ukladania správnych pokút 96
5. Skĺbenie právomocí vnútroštátnych dozorných orgánov s právomocami iných vnútroštátnych orgánov 99

I. Právo na ochranu osobných údajov uznané Chartou základných práv Európskej únie

1. Súlad sekundárneho práva Únie s právom na ochranu osobných údajov

Rozsudok z 9. novembra 2010 (veľká komora), Volker und Markus Schecke a Eifert (C-92/09 a C-93/09, EU:C:2010:662)

V tejto veci v rámci sporov vo veci samej vystupovali proti sebe na jednej strane poľnohospodári a na druhej strane Spolková krajina Hesensko vo veci uverejnenia osobných údajov, ktoré sa ich týkali ako príjemcov finančných prostriedkov z Európskeho poľnohospodárskeho záručného fondu (EPZF) a Európskeho poľnohospodárskeho fondu pre rozvoj vidieka (EPFRV), ktoré na svojej internetovej stránke uverejnil Bundesanstalt für Landwirtschaft und Ernährung (Spolkový úrad pre poľnohospodárstvo a výživu, Nemecko). Uvedení poľnohospodári namietali voči tomuto uverejneniu, pričom najmä tvrdili, že toto uverejnenie nebolo odôvodnené prevažujúcim verejným záujmom. Spolková krajina Hesensko sa domnievala, že uverejnenie uvedených údajov vyplývalo z nariadení (ES) č. 1290/2005[10] a č. 259/2008[11], ktoré upravujú financovanie spoločnej poľnohospodárskej politiky a ukladajú povinnosť uverejňovať informácie o fyzických osobách, ktoré sú prijímateľmi pomoci z EPZF a EPFRV.

Práve v tomto kontexte Verwaltungsgericht Wiesbaden (Správny súd Wiesbaden, Nemecko) položil Súdnemu dvoru viaceré otázky týkajúce sa platnosti niektorých ustanovení nariadenia (ES) č. 1290/2005 a nariadenia (ES) č. 259/2008, ktoré ukladajú povinnosť sprístupňovať verejnosti uvedené informácie, najmä na internetových stránkach spravovaných vnútroštátnymi orgánmi.

Súdny dvor v súvislosti s primeranosťou práva na ochranu osobných údajov, uznaného Chartou, a povinnosti transparentnosti v oblasti európskych fondov uviedol, že uverejňovanie údajov týkajúcich sa mien prijímateľov fondov a poskytovaných súm na internetovej stránke predstavuje vzhľadom na voľný prístup tretích osôb na stránku vo všeobecnosti zásah do práva dotknutých prijímateľov na ich súkromný život a osobitne do ochrany ich osobných údajov.

Na to, aby bolo možné takýto zásah odôvodniť, musí byť stanovený zákonom, rešpektovať podstatu týchto práv a podľa zásady proporcionality musí byť nevyhnutný

[10] Nariadenie Rady (ES) č. 1290/2005 z 21. júna 2005 o financovaní Spoločnej poľnohospodárskej politiky (Ú. v. EÚ L 209, 2005, s. 1), zrušené nariadením Európskeho parlamentu a Rady (EÚ) č. 1306/2013 zo 17. decembra 2013 o financovaní, riadení a monitorovaní spoločnej poľnohospodárskej politiky (Ú. v. EÚ L 347, 2013, s. 549).

[11] Nariadenie Komisie (ES) č. 259/2008 z 18. marca 2008, ktorým sa stanovujú podrobné pravidlá uplatňovania nariadenia Rady (ES) č. 1290/2005 v súvislosti s uverejňovaním informácií o prijímateľoch pomoci zo zdrojov EPZF a EPFRV (Ú. v. EÚ L 76, 2008, s. 28), zrušené vykonávacím nariadením Komisie (EÚ) č. 908/2014 zo 6. augusta 2014, ktorým sa stanovujú pravidlá uplatňovania nariadenia Európskeho parlamentu a Rady (EÚ) č. 1306/2013 vzhľadom na platobné agentúry a ostatné orgány, finančné hospodárenie, schvaľovanie účtovných závierok, pravidlá kontroly, zábezpeky a transparentnosť (Ú. v. EÚ L 255, 2014, s. 59).

a skutočne zodpovedať cieľom všeobecného záujmu, ktoré uznala Únia, pričom obmedzenia týchto práv sa musia vykonať v rámci toho, čo je striktne nevyhnutné. V tomto kontexte Súdny dvor usúdil, že hoci v demokratickej spoločnosti majú daňoví poplatníci právo byť informovaní o využívaní verejných finančných prostriedkov, nič to nemení na skutočnosti, že Rada a Komisia majú povinnosť vykonať vyvážené posúdenie dotknutých záujmov, čo si pred prijatím napadnutých právnych predpisov vyžadovalo preskúmať, či uverejnenie týchto údajov prostredníctvom jedinej internetovej stránky v členskom štáte nešlo nad rámec toho, čo je nevyhnutné na uskutočnenie sledovaných legitímnych cieľov.

Súdny dvor tak vyhlásil za neplatné niektoré ustanovenia nariadenia č. 1290/2005, ako aj nariadenia č. 259/2008 ako celku v rozsahu, v akom, pokiaľ ide o fyzické osoby – prijímateľov pomoci z EPZF a EPFRV –, tieto ustanovenia ukladajú povinnosť uverejňovať osobné údaje týkajúce sa všetkých prijímateľov bez toho, aby rozlišovali podľa relevantných kritérií, akými sú doba poskytovania pomoci, frekvencia poskytovania alebo druh a význam tejto pomoci. Súdny dvor však nespochybnil účinky uverejnenia zoznamov prijímateľov takejto pomoci, ku ktorému vnútroštátne orgány pristúpili v období predchádzajúcom dňu vyhlásenia rozsudku.

Rozsudok z 8. apríla 2014 (veľká komora), Digital Rights Ireland a Seitlinger a i. (spojené veci C-293/12 a C-594/12, EU:C:2014:238)

Základom tohto rozsudku sú návrhy na posúdenie platnosti smernice 2006/24/ES o uchovávaní údajov so zreteľom na základné práva na rešpektovania súkromného života a na ochranu osobných údajov, ktoré boli predložené v rámci vnútroštátnych sporov pred írskym a rakúskym vnútroštátnym súdom. Vo veci C-293/12 High Court (Vyšší súd, Írsko) rozhodoval spor medzi spoločnosťou Digital Rights a írskymi orgánmi vo veci zákonnosti vnútroštátnych opatrení týkajúcich sa uchovávania údajov súvisiacich s elektronickou komunikáciou. Vo veci C-594/12 Verfassungsgerichtshof (Ústavný súd, Rakúsko) rozhodoval o viacerých ústavných sťažnostiach smerujúcich k zrušeniu vnútroštátneho ustanovenia, ktorým sa do rakúskeho práva preberá smernica 2006/24.

Svojimi návrhmi na začatie prejudiciálneho konania sa írsky a rakúsky súd obrátili na Súdny dvor s otázkou platnosti smernice 2006/24 vzhľadom na články 7, 8 a 11 Charty. Konkrétnejšie uvedené súdy sa Súdneho dvora pýtali, či povinnosť podľa uvedenej smernice, uložená poskytovateľom verejne dostupných elektronických komunikačných služieb alebo verejných komunikačných sietí, a to uchovávať počas určitého obdobia údaje týkajúce sa súkromného života určitej osoby a jej komunikácie a sprístupniť ich príslušným vnútroštátnym orgánom, neprináša neopodstatnený zásah do uvedených základných práv. Dotknuté druhy údajov sú predovšetkým údaje potrebné na zistenie a identifikáciu zdroja komunikácie a adresáta komunikácie, na určenie dátumu, času, trvania a typu komunikácie, na identifikáciu komunikačného zariadenia užívateľa, ako aj na určenie polohy mobilného komunikačného zariadenia, teda údaje, ku ktorým patria predovšetkým meno a adresa účastníka alebo registrovaného užívateľa, telefónne číslo

volajúceho a číslo volaného, ako aj IP adresa pre internetové služby. Z týchto údajov predovšetkým vyplýva, s kým a akým spôsobom účastník alebo registrovaný užívateľ komunikoval, ako aj čas a miesto komunikácie. Okrem toho tieto údaje umožňujú zistiť, ako často účastník alebo registrovaný užívateľ komunikoval s určitými osobami v danom období.

Súdny dvor najskôr rozhodol, že ustanovenia smernice 2006/24 tým, že týmto poskytovateľom stanovujú takéto povinnosti, predstavujú osobitne závažný zásah do základných práv na rešpektovanie súkromného života a na ochranu osobných údajov, ktoré sú zaručené v článkoch 7 a 8 Charty. V tomto kontexte Súdny dvor nepochybne konštatoval, že tento zásah mohol byť odôvodnený sledovaním takého cieľa všeobecného záujmu, akým je boj proti organizovanému zločinu. Súdny dvor v tejto súvislosti v prvom rade uviedol, že uchovávanie údajov nariadené smernicou nie je spôsobilé zasiahnuť do podstaty základných práv na rešpektovanie súkromného života a na ochranu osobných údajov, keďže neumožňuje oboznámiť sa s obsahom samotnej elektronickej komunikácie, a upravuje, že poskytovatelia služieb alebo sietí musia dodržiavať určité zásady ochrany a bezpečnosti údajov. Súdny dvor v druhom rade uviedol, že uchovávanie údajov s ohľadom na ich prípadné postúpenie príslušným vnútroštátnym orgánom skutočne zodpovedá cieľu všeobecného záujmu, t. j. boju proti závažnej trestnej činnosti, a v konečnom dôsledku aj zabezpečeniu verejnej bezpečnosti.

Súdny dvor však usúdil, že prijatím smernice o uchovávaní údajov normotvorca Únie prekročil medze, ktoré vyžaduje dodržiavanie zásady proporcionality. V dôsledku toho vyhlásil smernicu za neplatnú, pričom usúdil, že zásah do základných práv, ktorý bol rozsiahly a obzvlášť závažný a ktorý upravovala táto smernica, nebol dostatočne vymedzený s cieľom zaistiť, že sa tento zásah obmedzí na to, čo je striktne nevyhnutné. Smernica 2006/24 totiž všeobecne zahŕňala akúkoľvek osobu a všetky spôsoby elektronickej komunikácie, ako aj všetky prevádzkové údaje bez toho, aby stanovovala akékoľvek rozlíšenie, obmedzenie alebo výnimku na základe cieľa, ktorým je boj proti závažnej trestnej činnosti. Smernica navyše neupravovala nijaké objektívne kritériá umožňujúce zabezpečiť, že príslušné vnútroštátne orgány by mali prístup k údajom a mohli ich použiť len na účely predchádzania, odhaľovania a trestného stíhania porušení, ktoré možno považovať za dostatočne závažné na odôvodnenie takéhoto zásahu, a nestanovila ani hmotnoprávne alebo procesnoprávne podmienky takéhoto prístupu alebo takéhoto použitia. Napokon, pokiaľ ide o dĺžku uchovávania údajov, smernica ukladala dobu najmenej šesť mesiacov bez akéhokoľvek rozlíšenia medzi jednotlivými kategóriami údajov v závislosti od dotknutých osôb alebo prípadnej užitočnosti údajov vo vzťahu k sledovanému cieľu.

Okrem toho, pokiaľ ide o požiadavky vyplývajúce z článku 8 ods. 3 Charty, Súdny dvor konštatoval, že smernica 2006/24 nestanovila dostatočné záruky umožňujúce zabezpečiť účinnú ochranu údajov pred rizikom zneužitia, ako aj pred nezákonným prístupom a použitím týchto údajov, a nestanovila ani uchovávanie údajov na území Únie.

V dôsledku toho uvedená smernica nezabezpečovala úplný dohľad nad dodržiavaním požiadaviek ochrany a bezpečnosti nezávislým orgánom tak, ako to výslovne vyžaduje Charta.

Rozsudok z 21. júna 2022 (veľká komora), Ligue des droits humains (C-817/19, EU:C:2022:491)

Údaje z PNR („Passenger Name Record“) sú informácie z rezervácií, ktoré leteckí dopravcovia uchovávajú v ich rezervačných systémoch a systémoch kontroly odletov. Smernica PNR[12] ukladá týmto dopravcom povinnosť poskytnúť údaje každého cestujúceho, ktorý využíva let mimo EÚ prevádzkovaný medzi treťou krajinou a Európskou úniou, útvaru informácií o cestujúcich („Passenger Information Unit“; ďalej len „PIU“) v členskom štáte príletu alebo odletu dotknutého letu na účely boja proti terorizmu a závažnej trestnej činnosti. Takto prenesené údaje z PNR sú totiž predmetom predbežného posúdenia zo strany PIU[13] a následne sa uchovávajú na účely prípadného neskoršieho posúdenia príslušnými orgánmi dotknutého členského štátu alebo iného členského štátu. Členské štáty sa môžu rozhodnúť, že budú uplatňovať túto smernicu aj na lety vnútri EÚ[14].

Neziskové združenie Ligue des droits humains (Liga pre ľudské práva) podalo na Cour constitutionnelle (Ústavný súd, Belgicko) žalobu o neplatnosť belgického zákona, ktorým sa do vnútroštátneho práva preberá tak smernica PNR, ako aj smernica API[15]. Podľa žalobcu tento zákon porušuje právo na rešpektovanie súkromného života a ochranu osobných údajov. Kritizuje na jednej strane veľmi široký charakter údajov PNR a na druhej strane všeobecnú povahu zhromažďovania, prenosu a spracovania takýchto údajov. Podľa neho zákon tiež narušuje voľný pohyb osôb tým, že nepriamo obnovuje hraničné kontroly rozšírením systému PNR na lety vnútri EÚ a na dopravu inými prostriedkami v rámci Únie.

V tomto kontexte sa belgický Cour constitutionnelle (Ústavný súd) obrátil na Súdny dvor s prejudiciálnymi otázkami, ktoré sa týkali najmä platnosti smernice PNR.

Súdny dvor rozsudkom vydaným veľkou komorou potvrdil platnosť smernice PNR v rozsahu, v akom ju možno vykladať v súlade s Chartou.

---

12 Smernica Európskeho parlamentu a Rady (EÚ) 2016/681 z 27. apríla 2016 o využívaní údajov zo záznamov o cestujúcich (PNR) na účely prevencie, odhaľovania, vyšetrovania a stíhania teroristických trestných činov a závažnej trestnej činnosti (Ú. v. EÚ L 119, 2016, s. 132) (ďalej len „smernica PNR“).

13 Cieľom tohto predbežného posúdenia je identifikovať osoby, ktoré by mali príslušné orgány ďalej preskúmať vzhľadom na to, že by sa mohli podieľať na teroristických trestných činoch alebo závažnej trestnej činnosti. Vykonáva sa systematicky a prostredníctvom automatizovaných prostriedkov tak, že údaje z PNR sa porovnávajú s databázami, „ktoré sú relevantné“, alebo sa spracúvajú na základe vopred stanovených kritérií v súlade s článkom 6 ods. 2 písm. a) a článkom 6 ods. 3 smernice PNR.

14 Využitím možnosti stanovenej v článku 2 smernice PNR.

15 Smernica Rady 2004/82/ES z 29. apríla 2004 o povinnosti dopravcov oznamovať údaje o cestujúcich (Ú. v. EÚ L 261, 2004, s. 24; Mim. vyd. 19/007, s. 74) (ďalej len „smernica API“). Táto smernica na účely zlepšenia hraničných kontrol a boja proti nelegálnemu prisťahovalectvu upravuje prenos vopred poskytovaných informácií o cestujúcich (ako sú napríklad číslo a typ použitého cestovného dokladu alebo štátna príslušnosť) leteckými dopravcami príslušným vnútroštátnym orgánom.

V tejto súvislosti Súdny dvor rozhodol, že keďže výklad ustanovení smernice PNR s ohľadom na články 7, 8 a 21, ako aj článok 52 ods. 1 Charty,[16] podaný Súdnym dvorom zabezpečuje súlad tejto smernice s týmito článkami, preskúmanie položených otázok neodhalilo nijakú skutočnosť, ktorá by mohla mať vplyv na platnosť uvedenej smernice.

Na úvod pripomenul, že akt Únie sa má vykladať, pokiaľ je to možné, spôsobom, ktorý nespochybní jeho platnosť, a v súlade s celým primárnym právom a najmä s ustanoveniami Charty, pričom členské štáty tak musia dbať na to, aby nevychádzali z výkladu tejto smernice, ktorý by bol v rozpore so základnými právami chránenými právnym poriadkom Únie alebo s inými všeobecnými zásadami uznanými v tomto právnom poriadku. Pokiaľ ide o smernicu PNR, Súdny dvor spresnil, že mnohé jej odôvodnenia a ustanovenia si vyžadujú takýto konformný výklad, pričom zdôrazňujú význam, ktorý normotvorca Únie prikladá s odkazom na vysokú úroveň ochrany údajov plnému dodržiavaniu základných práv zakotvených v Charte.

Súdny dvor konštatoval, že smernica PNR nepochybne prináša vážne zásahy do práv zaručených v článkoch 7 a 8 Charty, najmä v rozsahu, v akom sa snaží zaviesť nepretržitý, necielený a systematický režim dohľadu vrátane automatizovaného posudzovania osobných údajov všetkých osôb, ktoré využívajú služby leteckej dopravy. Pripomína, že možnosť členských štátov odôvodniť takýto zásah sa musí posudzovať prostredníctvom merania jeho závažnosti a overenia, či je dôležitosť sledovaného cieľa všeobecného záujmu priamo úmerná takejto závažnosti.

Súdny dvor dospel k záveru, že prenos, spracúvanie a uchovávanie údajov z PNR podľa tejto smernice možno považovať za obmedzené na to, čo je striktne nevyhnutné na účely boja proti teroristickým trestným činom a závažnej trestnej činnosti, za predpokladu, že právomoci stanovené v uvedenej smernici sa vykladajú reštriktívne. V tejto súvislosti rozsudok vydaný v tento deň okrem iného spresnil, že:

- Systém zavedený smernicou PNR sa musí vzťahovať len na jasne identifikovateľné a obmedzené informácie v rubrikách uvedených v prílohe I tejto smernice, ktoré súvisia s uskutočneným letom a dotknutým cestujúcim, čo v prípade niektorých rubrík tejto prílohy znamená, že sa tento systém vzťahuje len na údaje, ktoré sú v nich výslovne uvedené.[17]
- Uplatňovanie systému zavedeného smernicou PNR sa musí obmedziť na teroristické trestné činy a závažné formy trestnej činnosti, ktoré majú prinajmenšom nepriamo objektívnu súvislosť s leteckou prepravou cestujúcich. Pokiaľ ide o tieto formy, uplatňovanie tohto systému nemožno rozšíriť na trestné činy, ktoré síce spĺňajú kritérium stanovené v tejto smernici týkajúce sa hranice

[16] Podľa tohto ustanovenia akékoľvek obmedzenie výkonu práv a slobôd uznaných v Charte musí byť ustanovené zákonom a rešpektovať podstatu týchto práv a slobôd. Navyše tieto práva a slobody možno obmedziť len vtedy, ak je to nevyhnutné a skutočne to zodpovedá cieľom všeobecného záujmu, ktoré sú uznané Úniou, alebo ak je to potrebné na ochranu práv a slobôd iných.

[17] Najmä „informácie o spôsoboch platby“ (bod 6 prílohy) sa musia obmedziť na spôsoby platby a fakturácie letenky s vylúčením akýchkoľvek iných informácií, ktoré priamo nesúvisia s letom, a „všeobecné poznámky“ (bod 12) sa môžu týkať len informácií výslovne uvedených v tomto bode, ktoré sa týkajú maloletých cestujúcich.

závažnosti a sú uvedené v jej prílohe II, ale vzhľadom na osobitosti vnútroštátneho trestnoprávneho systému patria medzi bežnú trestnú činnosť.

– Prípadné rozšírenie uplatnenia smernice PNR na všetky lety vnútri EÚ alebo ich časť, o čom môže členský štát rozhodnúť využitím možnosti stanovenej v tejto smernici, sa musí obmedziť na to, čo je striktne nevyhnutné. Na tento účel musí toto uplatnenie podliehať účinnému preskúmaniu súdom alebo nezávislým správnym orgánom, ktorého rozhodnutie má záväzný účinok. V tejto súvislosti Súdny dvor spresnil, že:

  – Len v situácii, keď uvedený členský štát zistí, že existujú dostatočne konkrétne okolnosti na vyvodenie záveru, že čelí teroristickej hrozbe, ktorá sa javí ako skutočná a aktuálna alebo predvídateľná, neprekračuje uplatňovanie tejto smernice na všetky lety vnútri EÚ, ktoré do uvedeného členského štátu prilietajú alebo z neho odlietajú, časovo obmedzené na nevyhnutnú potrebu, ale s možnosťou predĺženia, rámec toho, čo je striktne nevyhnutné.[18]

  – V prípade neexistencie takejto teroristickej hrozby sa uplatňovanie uvedenej smernice nemôže rozšíriť na všetky lety vnútri EÚ, ale musí sa obmedziť na lety vnútri EÚ týkajúce sa najmä určitých leteckých spojení alebo schém cestovania či dokonca niektorých letísk, v súvislosti s ktorými podľa posúdenia dotknutého členského štátu existujú informácie, ktoré môžu odôvodniť takéto uplatňovanie. Striktná nevyhnutnosť tohto uplatňovania na takto vybrané lety vnútri EÚ sa musí pravidelne prehodnocovať vzhľadom na zmeny podmienok, ktoré odôvodnili ich výber.

– Na účely predbežného posúdenia údajov z PNR, ktorého cieľom je identifikácia osôb, v prípade ktorých sa vyžaduje ďalšie preskúmanie pred ich príchodom alebo odchodom a ktoré sa najskôr vykonáva prostredníctvom operácií automatizovaného spracúvania, môže PIU na jednej strane tieto údaje kontrolovať len v databázach týkajúcich sa hľadaných osôb alebo vecí, alebo osôb alebo vecí, na ktoré bol vydaný zápis.[19] Tieto databázy musia byť nediskriminačné a príslušné orgány ich musia využívať v súvislosti s bojom proti teroristickým trestným činom a závažnej trestnej činnosti, ktoré majú prinajmenšom nepriamo objektívnu súvislosť s leteckou prepravou cestujúcich. Pokiaľ ide na druhej strane o predbežné posúdenie na základe vopred stanovených kritérií, PIU nemôže používať technológie umelej inteligencie v rámci systémov strojového učenia

[18] Už samotná existencia takejto hrozby totiž môže vytvárať spojitosť medzi prenosom a spracúvaním dotknutých údajov na jednej strane a bojom proti terorizmu na strane druhej. Stanovenie uplatňovania smernice PNR na všetky lety vnútri EÚ s odletom alebo príletom do dotknutého členského štátu na obmedzené obdobie preto neprekračuje rámec toho, čo je striktne nevyhnutné, pričom rozhodnutie stanovujúce toto uplatňovanie musí byť možné preskúmať zo strany súdu alebo nezávislého správneho orgánu.

[19] Ide o databázy hľadaných osôb alebo vecí, alebo osôb alebo vecí, na ktoré bol vydaný zápis, v zmysle článku 6 ods. 3 písm. a) smernice PNR. Naproti tomu analýzy vychádzajúce z rôznych databáz môžu mať podobu získavania údajov („data mining“) a môžu viesť k neprimeranému využívaniu týchto údajov, a tým poskytnúť prostriedky na vytvorenie presného profilu dotknutých osôb len preto, lebo tieto osoby majú v úmysle cestovať lietadlom.

(„machine learning“), ktoré sú schopné bez ľudského zásahu a kontroly meniť proces posudzovania a najmä kritériá posudzovania, na ktorých je založený výsledok uplatňovania tohto procesu, ako aj zváženie týchto kritérií. Uvedené kritériá musia byť určované tak, aby sa ich uplatňovanie špecificky zameriavalo na osoby, v súvislosti s ktorými existuje dôvodné podozrenie z účasti na teroristických trestných činoch alebo závažnej trestnej činnosti a musia zohľadňovať skutočnosti svedčiace tak „v prospech“, ako aj „v neprospech“, bez toho, aby viedli k priamej alebo nepriamej diskriminácii.[20]

– Vzhľadom na mieru odchýlky spojenú s takýmto operáciami automatizovaného spracúvania údajov z PNR a pomerne veľký počet „falošne pozitívnych“ výsledkov, ktoré vyplynuli z ich uplatňovania v rokoch 2018 a 2019, vhodnosť systému zavedeného smernicou PNR na dosiahnutie sledovaných cieľov závisí najmä od riadneho fungovania overovania pozitívnych výsledkov získaných v rámci týchto operácií spracúvania, ktoré PIU následne vykonáva prostredníctvom neautomatizovaných prostriedkov. V tejto súvislosti musia členské štáty stanoviť jasné a presné pravidlá, ktoré môžu usmerniť a vymedziť analýzu vykonanú zástupcami PIU zodpovednými za toto individuálne preskúmanie, s cieľom zaručiť plné dodržiavanie základných práv zakotvených v článkoch 7, 8 a 21 Charty a najmä zabezpečiť jednotný administratívny postup v rámci PIU, ktorý rešpektuje zásadu nediskriminácie. Musia najmä zabezpečiť, že PIU stanoví objektívne kritériá preskúmania, ktoré umožnia jeho zástupcom overiť na jednej strane, či a v akom rozsahu sa pozitívna zhoda („hit“) skutočne týka jednotlivca, ktorý môže byť zapojený do teroristických trestných činov alebo závažnej trestnej činnosti, a na druhej strane nediskriminačnú povahu operácií automatizovaného spracúvania. V tejto súvislosti Súdny dvor tiež zdôraznil, že príslušné orgány musia zabezpečiť, aby dotknutá osoba bola schopná pochopiť fungovanie vopred stanovených kritérií posúdenia a programov uplatňujúcich tieto kritériá tak, aby sa mohla s plnou znalosťou veci rozhodnúť, či uplatní alebo neuplatní svoje právo na súdny prostriedok nápravy. Rovnako v rámci takéhoto opravného prostriedku musí mať súd zodpovedný za preskúmanie zákonnosti rozhodnutia prijatého príslušnými orgánmi, a s výnimkou prípadov ohrozenia bezpečnosti štátu aj samotná dotknutá osoba, možnosť oboznámiť sa so všetkými dôvodmi a dôkazmi, na základe ktorých bolo toto rozhodnutie prijaté, vrátane vopred stanovených kritérií posúdenia a fungovania programov uplatňujúcich tieto kritériá.
– Následné oznamovanie a posudzovanie údajov z PNR, t. j. po prílete alebo odlete dotknutej osoby, sa môže vykonať len na základe nových okolností a objektívnych skutočností, ktoré buď vyvolávajú dôvodné podozrenie z účasti tejto osoby na závažných formách trestnej činnosti, ktoré majú prinajmenšom nepriamo

[20] Vopred stanovené kritériá musia byť cielené, primerané a konkrétne a musia sa pravidelne preskúmavať (článok 6 ods. 4 smernice PNR). Predbežné posúdenie na základe vopred určených kritérií sa musí vykonávať nediskriminačným spôsobom. Podľa článku 6 ods. 4 štvrtej vety smernice PNR sa kritériá v žiadnom prípade nezakladajú na rasovom alebo etnickom pôvode osoby, jej politickom zmýšľaní, náboženskom vyznaní či filozofickom presvedčení, členstve v odborových organizáciách, zdraví, sexuálnom živote alebo sexuálnej orientácii.

objektívnu súvislosť s leteckou prepravou cestujúcich, alebo na základe ktorých sa možno domnievať, že tieto údaje môžu v konkrétnom prípade účinne prispieť k boju proti teroristickým trestným činom s takou súvislosťou. Sprístupnenie údajov z PNR na účely takéhoto následného posúdenia musí v zásade podliehať, s výnimkou náležite odôvodnených naliehavých prípadov, predchádzajúcemu preskúmaniu buď zo strany súdu, alebo nezávislého správneho orgánu na základe odôvodnenej žiadosti príslušných orgánov bez ohľadu na to, či bola táto žiadosť podaná pred uplynutím obdobia šiestich mesiacov po prenose týchto údajov útvaru PIU alebo po nej.[21]

Rozsudok z 22. novembra 2022 (veľká komora), Luxembourg Business Registers (C-37/20 a C-601/20, EU:C:2022:912)

Na účely boja a predchádzania praniu špinavých peňazí a financovaniu terorizmu smernica proti praniu špinavých peňazí[22] ukladá členským štátom povinnosť viesť register obsahujúci informácie o konečných užívateľoch výhod[23] podnikateľských subjektov a iných právnych subjektov, ktoré boli zaregistrované na ich území. V nadväznosti na zmenu tejto smernice smernicou 2018/843[24] musia byť niektoré z týchto informácií prístupné v každom prípade komukoľvek zo širokej verejnosti. V súlade s takto zmenenou smernicou proti praniu špinavých peňazí (ďalej len „zmenená smernica proti praniu špinavých peňazí“) luxemburská právna úprava zriadila Register konečných užívateľov výhod (ďalej len „RKUV“) určený na uchovanie a sprístupnenie celého radu informácií o konečných užívateľoch výhod zaregistrovaných subjektov, ku ktorým má ktokoľvek povolený prístup.

V tejto súvislosti boli na Tribunal d’arrondissement de Luxembourg (Okresný súd Luxemburg, Luxembursko) podané dve žaloby, a to WM a spoločnosťou Sovim SA, ktorými spochybnili zamietnutie, zo strany Luxembourg Business Registers, správcu RKUV, ich žiadostí o zabránenie prístupu širokej verejnosti k informáciám týkajúcim sa v prvom prípade WM ako konečného užívateľa výhod občianskoprávnej realitnej spoločnosti a v druhom prípade konečného užívateľa výhod, teda spoločnosti Sovim SA. V rámci týchto dvoch vecí Tribunal d’Arrondissement de Luxembourg (Okresný súd Luxemburg) položil Súdnemu dvoru prejudiciálnu otázku týkajúcu sa platnosti ustanovení práva Únie, ktorými sa zavádza systém verejného prístupu k informáciám týkajúcim sa konečných užívateľov výhod.

---

[21] Podľa článku 12 ods. 1 a 3 smernice PNR je takéto preskúmanie výslovne stanovené len v prípade žiadostí o sprístupnenie údajov z PNR podaných po uplynutí obdobia šiestich mesiacov po prenose týchto údajov PIU.

[22] Smernica Európskeho parlamentu a Rady (EÚ) 2015/849 z 20. mája 2015 o predchádzaní využívaniu finančného systému na účely prania špinavých peňazí alebo financovania terorizmu, ktorou sa mení nariadenie Európskeho parlamentu a Rady (EÚ) č. 648/2012 a zrušuje smernica Európskeho parlamentu a Rady 2005/60/ES a smernica Komisie 2006/70/ES (Ú. v. EÚ L 141, 2015, s. 73, ďalej len „smernica proti praniu špinavých peňazí“).

[23] Podľa článku 3 bodu 6 smernice proti praniu špinavých peňazí sú konečnými užívateľmi výhod akékoľvek fyzické osoby, ktoré skutočne ovládajú alebo vykonávajú kontrolu nad klientom, a/alebo fyzická(é) osoba(y), v mene ktorej(ých) sa transakcia alebo činnosť vykonáva.

[24] Smernica Európskeho parlamentu a Rady (EÚ) 2018/843 z 30. mája 2018, ktorou sa mení smernica (EÚ) 2015/849 o predchádzaní využívaniu finančného systému na účely prania špinavých peňazí alebo financovania terorizmu a smernice 2009/138/ES a 2013/36/EÚ (Ú. v. EÚ L 156, 2018, 43).

Súdny dvor zasadajúci vo veľkej komore vo svojom rozsudku konštatoval neplatnosť smernice 2018/843 v rozsahu, v akom táto smernica zmenila smernicu proti praniu špinavých peňazí v tom zmysle, že členské štáty musia zabezpečiť, aby informácie o konečných užívateľoch výhod a iných právnych subjektoch, ktoré boli zaregistrované na ich území, boli v každom prípade prístupné komukoľvek zo širokej verejnosti.[25]

Súdny dvor v prvom rade konštatoval, že prístup širokej verejnosti k informáciám o konečných užívateľoch výhod stanovený zmenenou smernicou proti praniu špinavých peňazí predstavuje vážny zásah do základných práv na rešpektovanie súkromného života a na ochranu osobných údajov, ktoré sú zakotvené v článkoch 7 a 8 Charty.

V tejto súvislosti Súdny dvor poznamenal, že vzhľadom na to, že dotknuté údaje obsahujú informácie o identifikovaných fyzických osobách, konkrétne o konečných užívateľoch výhod podnikateľských subjektov a iných právnych subjektov zaregistrovaných na území členských štátov, prístup kohokoľvek zo širokej verejnosti k týmto údajom má vplyv na základné právo na rešpektovanie súkromného života. Okrem toho ich sprístupnenie širokej verejnosti predstavuje spracovanie osobných údajov. Dodal, že takéto sprístupnenie širokej verejnosti predstavuje zásah do dvoch vyššie uvedených základných práv, bez ohľadu na ďalšie použitie poskytnutých informácií.

Pokiaľ ide o závažnosť tohto zásahu, Súdny dvor uviedol, že v rozsahu, v akom sa informácie sprístupnené širokej verejnosti týkajú totožnosti konečného užívateľa výhod, ako aj povahy a rozsahu jeho skutočných podielov v podnikateľských subjektoch alebo iných právnych subjektoch, je pravdepodobné, že umožnia profilovanie určitých osobných identifikačných údajov, stavu majetku dotknutej osoby, ako aj konkrétnych hospodárskych odvetví, krajín a podnikov, do ktorých táto osoba investovala. Tieto informácie sú navyše prístupné potenciálne neobmedzenému počtu osôb, a preto takéto spracovanie osobných údajov môže tiež umožniť, aby osoby, ktoré sa z dôvodov, ktoré nesúvisia s cieľom sledovaným týmto opatrením, chcú informovať najmä o materiálnej a finančnej situácii konečného užívateľa výhod, mali voľný prístup k uvedeným informáciám. Táto možnosť sa zdá o to jednoduchšia, ak údaje možno vyhľadať na internete. Okrem toho potenciálne dôsledky pre dotknuté osoby vyplývajúce z prípadného zneužitia ich údajov zhoršuje skutočnosť, že po sprístupnení širokej verejnosti tieto údaje môžu byť nielen voľne prístupné, ale aj uchovávané a šírené, a že sa pre tieto osoby stáva ešte ťažšie, dokonca až iluzórne účinne sa brániť proti zneužitiu.

V druhom rade Súdny dvor v rámci preskúmania odôvodnenia predmetného zásahu po prvé poznamenal, že v prejednávanej veci je dodržaná zásada zákonnosti. Obmedzenie výkonu vyššie spomenutých základných práv, ktoré vyplýva z prístupu širokej verejnosti k informáciám o konečných užívateľoch výhod, je totiž stanovené legislatívnym aktom, konkrétne zmenenou smernicou proti praniu špinavých peňazí. Okrem toho táto

[25] Neplatnosť článku 1 bodu 15 písm. c) smernice 2018/843, ktorou sa mení článok 30 ods. 5 prvý pododsek písm. c) smernice proti praniu špinavých peňazí.

smernica na jednej strane spresňuje, že tieto informácie musia byť primerané, presné a aktuálne, a výslovne vymenúva niektoré údaje, ku ktorým musí mať široká verejnosť umožnený prístup. Na druhej strane stanovuje podmienky, za ktorých môžu členské štáty stanoviť výnimky z takéhoto prístupu.

Po druhé spresnil, že predmetný zásah neohrozuje podstatu základných práv zaručených článkami 7 a 8 Charty. Hoci je pravda, že zmenená smernica proti praniu špinavých peňazí neobsahuje taxatívny výpočet údajov, ku ktorým musí byť komukoľvek zo širokej verejnosti povolený prístup, a že členské štáty môžu poskytnúť prístup k dodatočným informáciám, nič to nemení na tom, že jedine primerané informácie o konečných užívateľoch výhod a o držaných podieloch môžu byť získavané, uchovávané a v dôsledku toho potenciálne sprístupňované verejnosti, čo vylučuje najmä informácie, ktoré nemajú primeraný vzťah s cieľmi zmenenej smernice proti praniu špinavých peňazí. Nezdá sa však, že by sprístupnenie širokej verejnosti informácií, ktoré majú takýto vzťah, nejakým spôsobom ohrozilo podstatu uvedených základných práv.

Po tretie Súdny dvor zdôraznil, že normotvorca Únie tým, že upravil prístup širokej verejnosti k informáciám o konečných užívateľoch výhod, chce zabrániť praniu špinavých peňazí a financovaniu terorizmu tak, že prostredníctvom zvýšenej transparentnosti vytvorí prostredie, v ktorom bude menej pravdepodobné, že sa použije na tieto účely, čo predstavuje cieľ všeobecného záujmu, ktorý môže odôvodniť zásahy, hoci aj závažné, do základných práv zakotvených v článkoch 7 a 8 Charty.

Po štvrté v rámci preskúmania spôsobilej, nevyhnutnej a primeranej povahy predmetného zásahu Súdny dvor konštatoval, že je pravda, že prístup širokej verejnosti k informáciám o konečných užívateľoch výhod môže prispieť k dosiahnutiu tohto cieľa.

Domnieva sa však, že tento zásah nemožno považovať za obmedzený na to, čo je striktne nevyhnutné. Na jednej strane striktnú nevyhnutnosť uvedeného zásahu nemožno preukázať na základe skutočnosti, že kritérium „legitímneho záujmu“, ktorý musela mať podľa smernice proti praniu špinavých peňazí v znení pred jej zmenou smernicou 2018/843 každá osoba, ktorá chcela mať prístup k informáciám o konečných užívateľoch výhod, bolo ťažko uplatniteľné a že jeho uplatnenie mohlo viesť k svojvoľným rozhodnutiam. Prípadná existencia ťažkostí s presným vymedzením predpokladov a podmienok, za ktorých môže mať verejnosť prístup k informáciám o konečných užívateľoch výhod, totiž nemôže odôvodniť to, aby normotvorca Únie stanovil prístup širokej verejnosti k týmto informáciám.

Na druhej strane vysvetlenia uvedené v smernici 2018/843 tiež nemôžu preukázať striktnú nevyhnutnosť predmetného zásahu.[26] V rozsahu, v akom podľa týchto vysvetlení prístup širokej verejnosti k informáciám o konečných užívateľoch výhod má za cieľ umožniť väčšiu kontrolu informácií občianskou spoločnosťou, najmä zo strany tlače alebo organizácií občianskej spoločnosti, Súdny dvor uviedol, že tak tlač, ako aj

[26] Týka sa to vysvetlení uvedených v odôvodnení 30 smernice 2018/843.

organizácie občianskej spoločnosti, ktoré sa spájajú s predchádzaním a bojom proti praniu špinavých peňazí a financovaniu terorizmu, majú legitímny záujem na prístupe k dotknutým informáciám. To isté platí pre osoby, ktoré chcú poznať totožnosť konečných užívateľov výhod podnikateľských subjektov alebo iných právnych subjektov z dôvodu, že môžu s nimi uzavrieť transakcie, alebo aj pre finančné inštitúcie a orgány podieľajúce sa na boji proti porušeniam v oblasti prania špinavých peňazí alebo financovania terorizmu.

Okrem toho predmetný zásah tiež nie je primeraný. V tejto súvislosti Súdny dvor konštatoval, že hmotnoprávne pravidlá upravujúce tento zásah nezodpovedajú požiadavke jasnosti a presnosti. Zmenená smernica proti praniu špinavých peňazí totiž stanovuje prístup kohokoľvek zo širokej verejnosti „aspoň“ k údajom, ktoré sú v nej uvedené, a umožňuje členským štátom poskytnúť prístup k dodatočným informáciám, ktoré zahŕňajú „aspoň“ dátum narodenia alebo kontaktné údaje dotknutého konečného užívateľa výhod. Použitím výrazu „aspoň“ táto smernica umožňuje sprístupniť verejnosti údaje, ktoré nie sú dostatočne definované ani identifikovateľné.

Okrem toho, pokiaľ ide o vyváženie závažnosti tohto zásahu s významom sledovaného cieľa všeobecného záujmu, Súdny dvor uznal, že tento cieľ môže vzhľadom na svoj význam odôvodniť zásahy, a to aj závažné, do základných práv zakotvených v článkoch 7 a 8 Charty.

Na jednej strane však boj proti praniu špinavých peňazí a financovaniu terorizmu je predovšetkým záležitosťou orgánov verejnej moci, ako aj subjektov, akými sú úverové alebo finančné inštitúcie, ktoré z dôvodu svojej činnosti podliehajú osobitným povinnostiam v tejto oblasti. Z tohto dôvodu zmenená smernica proti praniu špinavých peňazí stanovuje, že informácie o konečných užívateľoch výhod musia byť prístupné v každom prípade príslušným orgánom a finančným spravodajským jednotkám, a to bez obmedzenia, ako aj povinným subjektom, v rámci povinnej starostlivosti vo vzťahu ku klientovi.[27]

Na druhej strane v porovnaní s predchádzajúcim režimom, ktorý okrem prístupu príslušných orgánov a určitých subjektov k informáciám o konečných užívateľoch výhod stanovoval aj prístup každej osoby alebo organizácie, ktorá môže preukázať legitímny záujem, režim zavedený smernicou 2018/843 predstavuje podstatne závažnejší zásah do základných práv zaručených článkami 7 a 8 Charty, bez toho, aby toto zhoršenie mohlo byť vyvážené prípadnými výhodami, ktoré by mohli vyplynúť z tohto posledného uvedeného režimu v porovnaní s prvým, pokiaľ ide o boj proti praniu špinavých peňazí a financovaniu terorizmu.

[27] Článok 30 ods. 5 prvý pododsek písm. a) a b) zmenenej smernice proti praniu špinavých peňazí.

2. Dodržiavanie práva na ochranu osobných údajov v rámci vykonávania práva Únie

Rozsudok z 21. decembra 2016 (veľká komora), Tele2 Sverige (spojené veci C-203/15 a C-698/15, EU:C:2016:970***)***

V nadväznosti na rozsudok Digital Rights Ireland a Seitlinger a i., ktorým bola smernica 2006/24 (pozri vyššie) vyhlásená za neplatnú, Súdny dvor rozhodoval o dvoch veciach týkajúcich sa všeobecnej povinnosti, ktorá je vo Švédsku a v Spojenom kráľovstve uložená poskytovateľom elektronických komunikačných služieb, a to uchovávať údaje týkajúce sa týchto komunikácií, ktorých uchovávanie upravovala už neplatná smernica.

Deň po vyhlásení rozsudku Digital Rights Ireland a Seitlinger a i. telekomunikačný podnik Tele2 Sverige oznámil švédskemu orgánu pre dohľad nad poštami a telekomunikáciami svoje rozhodnutie, že nebude viac uchovávať údaje, ako aj svoj zámer vymazať údaje, ktoré už boli zaregistrované (vec C-203/15). Švédske právo totiž ukladalo poskytovateľom elektronických komunikačných služieb povinnosť systematicky a priebežne, a to bez výnimky, uchovávať všetky údaje o prenose dát a polohe všetkých účastníkov a registrovaných užívateľov, týkajúce sa všetkých prostriedkov elektronickej komunikácie. Vo veci C-698/15 podali tri osoby žaloby proti britskému režimu uchovávania údajov, ktorý umožňoval, aby minister vnútra vyžadoval od prevádzkovateľov verejných telekomunikačných služieb uchovávanie všetkých údajov týkajúcich sa komunikácií, a to počas obdobia najviac 12 mesiacov, pričom uchovávanie obsahu týchto komunikácií bolo vylúčené.

Kammarrätten i Stockholm (Odvolací správny súd Štokholm, Švédsko) a Court of Appeal (England and Wales) (Civil Division) [Odvolací súd (Anglicko a Wales) (občianskoprávny senát), Spojené kráľovstvo] požiadali Súdny dvor, aby sa vyjadril k výkladu článku 15 ods. 1 smernice 2002/58, tzv. „smernice o súkromí a elektronických komunikáciách“, ktorý členským štátom umožňuje, aby stanovili určité výnimky z povinnosti uvedenej v tejto smernici, a to zabezpečiť dôvernosť elektronických komunikácií a príslušných údajov o prenose dát.

Vo svojom rozsudku Súdny dvor najskôr rozhodol, že článok 15 ods. 1 smernice 2002/58 v spojení s článkami 7, 8 a 11, ako aj s článkom 52 ods. 1 Charty bráni takej vnútroštátnej právnej úprave, akou je právna úprava Švédska, ktorá na účely boja proti trestnej činnosti stanovuje všeobecné a nediferencované uchovávanie všetkých údajov o prenose dát a polohe všetkých účastníkov a registrovaných užívateľov týkajúce sa všetkých prostriedkov elektronickej komunikácie. Podľa Súdneho dvora takáto právna úprava ide nad rámec toho, čo je striktne nevyhnutné, a nemožno ju považovať za odôvodnenú v demokratickej spoločnosti, ako to vyžaduje uvedený článok 15 ods. 1 v spojení s už citovanými článkami Charty.

To isté ustanovenie v spojení s tými istými článkami Charty rovnako bráni vnútroštátnej právnej úprave, ktorá upravuje ochranu a bezpečnosť údajov o prenose dát a polohe, najmä prístup príslušných vnútroštátnych orgánov k uchovávaným údajom, avšak tento prístup v rámci boja proti trestnej činnosti neobmedzuje len na účely boja proti závažnej trestnej činnosti, nepodmieňuje uvedený prístup predbežnému preskúmaniu zo strany súdu alebo nezávislého správneho orgánu a nevyžaduje, aby sa predmetné údaje uchovávali na území Únie.

Naproti tomu Súdny dvor usúdil, že článok 15 ods. 1 smernice 2002/58 nebráni právnej úprave, ktorá preventívne umožňuje, aby sa cielene uchovávali údaje tejto povahy na účely boja proti závažnej trestnej činnosti pod podmienkou, že sa toto uchovávanie údajov, pokiaľ ide o kategórie dotknutých údajov, príslušné komunikačné prostriedky, dotknuté osoby, ako aj dĺžku doby uchovávania, obmedzí na to, čo je striktne nevyhnutné. Na splnenie týchto požiadaviek musí táto vnútroštátna právna úprava stanoviť v prvom rade jasné a presné pravidlá umožňujúce účinne chrániť údaje pred rizikami zneužitia. Táto právna úprava musí najmä uvádzať okolnosti a podmienky, za ktorých môže byť opatrenie na uchovávanie údajov preventívne prijaté, čím sa zabezpečí, že také opatrenie sa obmedzí na to, čo je striktne nevyhnutné. V druhom rade, pokiaľ ide o hmotnoprávne podmienky, ktoré musí spĺňať vnútroštátna právna úprava s cieľom zabezpečiť, aby sa obmedzovala na to, čo je striktne nevyhnutné, uchovávanie údajov musí vždy zodpovedať objektívnym kritériám, ktoré zodpovedajú vzťahu medzi uchovávanými údajmi a sledovaným cieľom. Konkrétne takéto podmienky sa musia v praxi javiť ako spôsobilé skutočne vymedziť rozsah opatrenia a v dôsledku toho aj dotknutú verejnosť. Pokiaľ ide o toto vymedzenie, vnútroštátna právna úprava sa musí zakladať na objektívnych skutočnostiach, 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.

II. Spracovanie osobných údajov v zmysle všeobecnej právnej úpravy v danej oblasti

1. Pôsobnosť všeobecnej právnej úpravy

Rozsudok z 30. mája 2006 (veľká komora), Parlament/Rada (C-317/04 a C-318/04, EU:C:2006:346)

Po teroristických útokoch z 11. septembra 2001 prijali Spojené štáty právnu úpravu, ktorá stanovila, že leteckí prepravcovia zabezpečujúci leteckú dopravu z, do alebo cez územie Spojených štátov sú povinní poskytnúť americkým orgánom elektronický prístup

k údajom uvedeným v ich rezervačných systémoch a systémoch kontroly odletov, označeným ako „Passenger Name Records“ (PNR).

Keďže sa Komisia domnievala, že tieto ustanovenia by mohli byť v rozpore s európskou právnou úpravou a právnou úpravou členských štátov v oblasti ochrany údajov, začala rokovania s americkými orgánmi. V nadväznosti na tieto rokovania prijala Komisia 14. mája 2004 rozhodnutie 2004/535/ES[28], v ktorom sa konštatovalo, že Úrad Spojených štátov na ochranu colného priestoru a hraníc (United States Bureau of Customs and Border Protection, ďalej len „CBP“) zabezpečuje primeranú úroveň ochrany údajov z PNR prenášaných zo Spoločenstva (ďalej len „rozhodnutie o primeranosti“). Rada následne 17. mája 2004 prijala rozhodnutie 2004/496/ES[29], ktorým bolo schválené uzavretie dohody medzi Európskym spoločenstvom a Spojenými štátmi o spracovaní a postúpení údajov z PNR leteckými dopravcami usadenými na území členských štátov Spoločenstva.

Európsky parlament požiadal Súdny dvor, aby zrušil obe uvedené rozhodnutia, pričom najmä tvrdil, že rozhodnutie o primeranosti bolo prijaté *ultra vires*, že článok 95 ES (teraz článok 114 ZFEÚ) nepredstavuje vhodný právny základ pre rozhodnutie o schválení uzavretia dohody a že v oboch prípadoch došlo k porušeniu základných práv.

Pokiaľ ide o rozhodnutie o primeranosti, Súdny dvor najskôr preskúmal, či Komisia mohla oprávnene prijať svoje rozhodnutie na základe smernice 95/46. V tomto kontexte konštatoval, že z rozhodnutia o primeranosti vyplýva, že prenos údajov z PNR do CBP predstavuje spracovanie, ktorého cieľom je verejná bezpečnosť a iné štátne činnosti týkajúce sa oblasti trestného práva. Podľa Súdneho dvora, hoci boli údaje z PNR najprv zhromaždené leteckými spoločnosťami v rámci činnosti, ktorá patrí do pôsobnosti práva Únie, a to konkrétne v rámci predaja letenky, ktorý zakladá nárok na poskytnutie služby, spracovanie údajov, ktorého sa týkalo rozhodnutie o primeranosti, malo úplne inú povahu. Toto rozhodnutie sa totiž netýkalo spracovania údajov nevyhnutného na poskytnutie služby, ale spracovania údajov, ktoré sa považuje za nevyhnutné na zabezpečenie verejnej bezpečnosti a na represívne účely.

Súdny dvor v tejto súvislosti uviedol, že skutočnosť, že údaje z PNR zhromažďovali súkromní podnikatelia na komerčné účely a že títo podnikatelia zabezpečovali ich prenos do tretieho štátu, nebránila tomu, aby sa tento prenos považoval za spracovanie údajov, ktoré je vylúčené z pôsobnosti smernice. Tento prenos totiž patril do rámca vytvoreného orgánmi verejnej moci na účely verejnej bezpečnosti. Súdny dvor preto dospel k záveru, že rozhodnutie o primeranosti nepatrí do pôsobnosti smernice, lebo sa týka spracovania osobných údajov, ktoré je z tejto pôsobnosti vylúčené. Súdny dvor v dôsledku toho rozhodnutie o primeranosti zrušil.

[28] Rozhodnutie Komisie 2004/535/ES zo 14. mája 2004 o adekvátnej ochrane osobných údajov uvedených v Zázname podľa mena cestujúceho o cestujúcich lietadlom odoslaných Úradu Spojených štátov na ochranu colného priestoru a hraníc (Ú. v. EÚ L 235, 2004, s. 11).

[29] Rozhodnutie Rady 2004/496/ES zo 17. mája 2004 o uzavretí dohody medzi Európskym spoločenstvom a Spojenými štátmi americkými o spracovaní a postúpení údajov PNR leteckými dopravcami Úradu pre colnú správu a ochranu hraníc Ministerstva vnútornej bezpečnosti Spojených štátov amerických (Ú. v. EÚ L 183, 2004, s. 83).

Pokiaľ ide o rozhodnutie Rady, Súdny dvor konštatoval, že článok 95 ES v spojení s článkom 25 smernice 95/46 neumožňuje založiť právomoc Spoločenstva na účely uzavretia dotknutej dohody so Spojenými štátmi. Táto dohoda sa totiž týkala toho istého prenosu údajov ako rozhodnutie o primeranosti, a teda spracovania údajov, ktoré je vylúčené z pôsobnosti smernice. Súdny dvor v dôsledku toho zrušil rozhodnutie Rady o schválení uzavretia dohody.

Rozsudok z 13. mája 2014 (veľká komora), Google Spain a Google (C-131/12, EU:C:2014:317)

V roku 2010 španielsky štátny príslušník podal na Agencia Española de Protección de Datos (Španielska agentúra na ochranu údajov, ďalej len „AEPD“) sťažnosť proti vydavateľovi denníka rozširovaného vo veľkom rozsahu v Španielsku La Vanguardia Ediciones SL, ako aj proti spoločnostiam Google Spain a Google. Táto osoba tvrdila, že keď ako používateľ internetu zadá svoje meno do vyhľadávača skupiny Google, zoznam výsledkov zobrazí odkazy na dve stránky denníka La Vanguardia z roku 1998 oznamujúce najmä predaj nehnuteľností na dražbe, ktorý sa organizoval v nadväznosti na uplatnenie záložného práva s cieľom vymáhať dlhy tejto osoby. Svojou sťažnosťou táto osoba po prvé žiadala, aby sa vydavateľovi La Vanguardia nariadilo buď vymazať alebo zmeniť uvedené stránky, alebo aby tento vydavateľ využil niektoré nástroje poskytované vyhľadávačmi s cieľom chrániť tieto údaje. Po druhé uvedená osoba žiadala, aby sa spoločnostiam Google Spain alebo Google nariadilo vymazať alebo skryť jej osobné údaje tak, aby sa už neobjavovali vo výsledkoch vyhľadávania a v odkazoch na La Vanguardia.

AEPD zamietla sťažnosť smerujúcu proti vydavateľovi La Vanguardia, keďže sa domnievala, že tento vydavateľ uverejnil dotknuté informácie v súlade s právnymi predpismi, avšak pokiaľ išlo o spoločnosti Google Spain a Google, sťažnosti vyhovela, pričom tieto dve spoločnosti požiadala, aby prijali nevyhnutné opatrenia na stiahnutie údajov zo svojich indexov a na znemožnenie prístupu k nim v budúcnosti. Vzhľadom na to, že uvedené spoločnosti podali dve žaloby na Audiencia Nacional (Národný vyšší súd, Španielsko), v ktorých navrhovali zrušiť rozhodnutie AEPD, španielsky súd sa obrátil na Súdny dvor so sériou otázok.

V tomto rozsudku sa Súdny dvor tiež vyjadril k územnej pôsobnosti smernice 95/46.

Súdny dvor tak rozhodol, že spracovanie osobných údajov sa uskutočňuje v rámci činností prevádzkarne prevádzkovateľa tohto spracovania osobných údajov na území určitého členského štátu v zmysle smernice 95/46, ak poskytovateľ vyhľadávača, hoci má svoje sídlo v treťom štáte, založí v členskom štáte pobočku alebo dcérsku spoločnosť určenú na zaručenie podpory a predaja reklamného priestoru ponúkaného týmto vyhľadávačom, ktorá zameriava svoju činnosť na obyvateľov tohto členského štátu.

Za takých okolností totiž činnosti prevádzkovateľa vyhľadávača a činnosti jeho prevádzkarne nachádzajúcej sa v dotknutom členskom štáte, hoci sa odlišujú, sú neoddeliteľne spojené, keďže činnosti týkajúce sa reklamného priestoru predstavujú

prostriedok, v dôsledku ktorého sa dotknutý vyhľadávač stáva hospodársky výnosný, pričom tento vyhľadávač je súčasne prostriedkom, ktorý umožňuje vykonanie týchto činností.

Rozsudok z 11. decembra 2014, Ryneš (C-212/13, EU:C:2014:2428)

V reakcii na opakované protiprávne konania nainštaloval pán Ryneš na svoj dom bezpečnostnú kameru. Po ďalšom útoku na jeho dom bolo možné na základe záznamu z uvedeného kamerového systému identifikovať dve podozrivé osoby, voči ktorým sa začalo trestné konanie. Vzhľadom na to, že jeden z podozrivých napadol pred českým Úradom na ochranu osobných údajov zákonnosť spracovania údajov zaznamenaných kamerovým systémom, tento Úrad konštatoval, že pán Ryneš porušil právne predpisy v oblasti ochrany osobných údajov, a uložil mu pokutu.

Nejvyšší správní soud (Česká republika), na ktorý pán Ryneš podal kasačný opravný prostriedok smerujúci proti rozhodnutiu, ktoré vydal Městský soud v Praze (Česká republika) a ktorým bolo potvrdené rozhodnutie Úradu, položil Súdnemu dvoru otázku, či záznam vykonaný pánom Rynešom na účely ochrany jeho života, zdravia a majetku predstavuje spracovanie údajov, na ktoré sa smernica 95/46 nevzťahuje, lebo ide o záznam vykonaný fyzickou osobou na výkon výlučne osobných alebo domácich činností v zmysle článku 3 ods. 2 druhej zarážky uvedenej smernice.

Súdny dvor rozhodol, že prevádzkovanie kamerového systému umiestneného fyzickou osobou na jej rodinnom dome na účely ochrany majetku, zdravia a života majiteľov domu, ktorý umožňuje obrazový záznam osôb ukladaný do nahrávacieho zariadenia, na ktorom sa záznam priebežne nahráva na harddisk, pričom tento systém sníma tiež verejné priestranstvo, nepredstavuje spracovanie údajov na výkon výlučne osobných alebo domácich činností.

V tejto súvislosti pripomenul, že ochrana základného práva na súkromný život zaručeného v článku 7 Charty vyžaduje, aby výnimky a obmedzenia v súvislosti s ochranou osobných údajov nepôsobili nad rámec toho, čo je striktne nevyhnutné. Keďže ustanovenia smernice 95/46 sa majú v rozsahu, v akom upravujú spracovanie osobných údajov, ktoré môže viesť k porušeniu základných slobôd a predovšetkým práva na súkromný život, nevyhnutne vykladať s prihliadnutím na základné práva, ktoré sú zapísané v uvedenej Charte, výnimku stanovenú v článku 3 ods. 2 druhej zarážke tejto smernice treba vykladať reštriktívne. Navyše samotné znenie tohto ustanovenia vylučuje z uplatnenia smernice 95/46 spracovanie údajov uskutočnené na výkon „výlučne“ osobných alebo domácich činností. V rozsahu, v akom kamerový systém sníma, hoci len čiastočne, verejné priestranstvo a smeruje mimo súkromnú sféru osoby, ktorá jeho prostredníctvom spracúva údaje, nemožno ho považovať za výlučne „osobnú či domácu“ činnosť v zmysle uvedeného ustanovenia.

Rozsudok zo 16. januára 2024 (veľká komora), Österreichische Datenschutzbehörde (C-33/22, EU:C:2024:46)

S cieľom preskúmať prípadné politické ovplyvňovanie Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (Spolkový úrad pre ochranu ústavy a boj proti terorizmu, Rakúsko)[30], zriadila Nationalrat (Národná rada, Rakúsko) vyšetrovací výbor (ďalej len „vyšetrovací výbor BVT“). Tento výbor vypočul WK ako svedka. Napriek jeho žiadosti o anonymizáciu bola zápisnica z jeho vypočutia, v ktorej boli uvedené jeho celé priezvisko a meno, uverejnená na internetovej stránke Parlament Österreich (Rakúsky parlament). WK podal sťažnosť na Österreichische Datenschutzbehörde (Úrad na ochranu údajov, Rakúsko) (ďalej len „Datenschutzbehörde“), pričom tvrdil, že takéto uverejnenie jeho totožnosti je v rozpore s GDPR a rakúskou právnou úpravou. Rozhodnutím z 18. septembra 2019 Datenschutzbehörde vyhlásil, že nemá právomoc rozhodnúť o sťažnosti, pričom vysvetlil, že zásada deľby moci vylučuje, aby ako orgán výkonnej moci mohol kontrolovať vyšetrovací výbor BVT, ktorý patrí do zákonodarnej moci.

V nadväznosti na rozhodnutie Bundesverwaltungsgericht (Spolkový správny súd, Rakúsko), ktorým sa vyhovelo žalobe WK a zrušilo rozhodnutie Datenschutzbehörde, podal WK na Najvyšší správny súd opravný prostriedok „Revision“ proti rozhodnutiu spolkového správneho súdu.

V tomto kontexte sa vnútroštátny súd pýta Súdneho dvora, či činnosti vyšetrovacieho výboru zriadeného parlamentom členského štátu patria do pôsobnosti GDPR a či sa toto nariadenie uplatňuje v prípade, keď sa tieto činnosti týkajú ochrany národnej bezpečnosti.

V prvom rade Súdny dvor pripomenul, že jediným cieľom článku 2 ods. 2 písm. a) GDPR, ktorý stanovuje, že toto nariadenie sa nevzťahuje na spracúvanie osobných údajov v rámci činnosti, ktorá nepatrí do pôsobnosti práva Únie, je vylúčiť z jeho pôsobnosti spracúvanie vykonávané štátnymi orgánmi v rámci činnosti, ktorej cieľom je chrániť národnú bezpečnosť, alebo činnosti, ktorá patrí do tej istej kategórie. Samotná skutočnosť, že ide o činnosť štátu alebo orgánu verejnej moci, tak nestačí na automatické vylúčenie uplatňovania GDPR na takúto činnosť.

Tento výklad vyplývajúci z neexistencie rozlišovania v závislosti od totožnosti dotknutého prevádzkovateľa potvrdzuje článok 4 bod 7 GDPR.[31]

Súdny dvor spresňuje, že parlamentná povaha vyšetrovacieho výboru BVT neznamená, že jeho činnosti sú vylúčené z pôsobnosti GDPR. Výnimka stanovená v článku 2 ods. 2 písm. a) tohto nariadenia sa totiž vzťahuje len na kategórie činností, ktoré vzhľadom na

[30] Dňa 1. decembra 2021 bol tento subjekt nahradený „Direktion Staatsschutz und Nachrichtendienst“ (Riaditeľstvo pre bezpečnosť štátu a spravodajské služby, Rakúsko).

[31] Podľa tohto článku je zadefinovaný pojem „prevádzkovateľ“ ako „fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt, ktorý sám alebo spoločne s inými určí účely a prostriedky spracúvania osobných údajov“.

svoju povahu nepatria do pôsobnosti práva Únie, a nie na kategórie osôb. Okolnosť, že spracúvanie osobných údajov vykonáva vyšetrovací výbor zriadený parlamentom členského štátu pri výkone jeho kontrolnej právomoci výkonnej moci, sama osebe neumožňuje konštatovať, že toto spracúvanie sa vykonáva v rámci činnosti, ktorá nepatrí do pôsobnosti práva Únie.

V druhom rade Súdny dvor uvádza, že síce členským štátom prináleží definovať ich základné bezpečnostné záujmy a prijať opatrenia vhodné na ich zabezpečenie,[32] samotná skutočnosť, že vnútroštátne opatrenie bolo prijaté na účely ochrany národnej bezpečnosti, nemôže mať za následok neuplatniteľnosť práva Únie a oslobodiť členské štáty od potrebného dodržiavania tohto práva. Výnimka stanovená v článku 2 ods. 2 písm. a) GDPR pritom odkazuje len na kategórie činností, ktoré vzhľadom na svoju povahu nepatria do pôsobnosti práva Únie. V tejto súvislosti okolnosť, že prevádzkovateľom je orgán verejnej moci, ktorého hlavnou činnosťou je zabezpečiť národnú bezpečnosť, nemôže sama osebe postačovať na to, aby bolo z pôsobnosti GDPR vylúčené spracovanie osobných údajov, ktoré vykonáva v rámci svojich ostatných činností.

V prejednávanej veci sa zdá, že politická kontrola vykonaná vyšetrovacím výborom BVT sama osebe nepredstavuje činnosť smerujúcu k ochrane národnej bezpečnosti alebo patriacu do tej istej kategórie. Preto s výhradou overenia vnútroštátnym súdom nie je táto činnosť vyňatá z pôsobnosti GDPR.

Parlamentný vyšetrovací výbor však môže mať prístup k osobným údajom, na ktoré sa z dôvodov súvisiacich s národnou bezpečnosťou musí vzťahovať osobitná ochrana. V tejto súvislosti možno prostredníctvom legislatívnych opatrení stanoviť obmedzenia práv a povinností vyplývajúcich z GDPR najmä na účely zabezpečenia národnej bezpečnosti.[33] Na tomto základe by tak mohli byť odôvodnené obmedzenia týkajúce sa zhromažďovania osobných údajov, informovania dotknutých osôb a ich prístupu k uvedeným údajom, ako aj ich sprístupnenia bez súhlasu dotknutých osôb iným osobám, než je prevádzkovateľ, pod podmienkou, že rešpektujú podstatu základných práv a slobôd dotknutých osôb a predstavujú nevyhnutné a primerané opatrenie v demokratickej spoločnosti.

Súdny dvor však poznamenáva, že z informácií, ktoré má k dispozícii, nevyplýva, že vyšetrovací výbor BVT tvrdil, že uverejnenie osobných údajov dotknutej osoby bolo nevyhnutné na ochranu národnej bezpečnosti a bolo založené na vnútroštátnom legislatívnom opatrení stanovenom na tento účel, čo musí prípadne overiť vnútroštátny súd.

[32] V súlade s článkom 4 ods. 2 ZEÚ.
[33] Podľa článku 23 GDPR.

2. Pojem „osobné údaje“

Rozsudok z 19. októbra 2016, Breyer (C-582/14, EU:C:2016:779)

Pán Breyer podal na nemecké občianskoprávne súdy žalobu smerujúcu k tomu, aby bol Spolkovej republike Nemecko uložený zákaz uchovávať, a to aj prostredníctvom tretích strán, informatické údaje, ktoré boli prenesené po skončení každého prehliadania internetových stránok nemeckých spolkových orgánov. S cieľom zabrániť útokom a umožniť stíhanie útočníkov poskytovateľ online mediálnych služieb nemeckých spolkových orgánov totiž uchovával údaje spočívajúce v „dynamickej“ IP adrese – t. j. IP adrese, ktorá sa mení pri každom novom internetovom pripojení –, ako aj v dátume a čase prehliadania internetovej stránky. Na rozdiel od statických IP adries dynamické IP adresy *a priori* neumožňujú vytvoriť na základe verejne prístupných súborov spojenie medzi určitým počítačom a fyzickým pripojením do siete používanej poskytovateľom internetového prístupu. Uchované údaje samy osebe neposkytovali poskytovateľovi online mediálnych služieb možnosť identifikovať používateľa. Naproti tomu poskytovateľ internetového pripojenia mal k dispozícii dodatočné informácie, ktoré po ich spojení s touto IP adresou umožňovali identifikovať uvedeného používateľa.

V tomto kontexte Bundesgerichtshof (Spolkový súdny dvor, Nemecko), ktorý rozhodoval o opravnom prostriedku „Revision“, položil Súdnemu dvoru otázku, či IP adresa, ktorú poskytovateľ online mediálnych služieb uchováva v súvislosti s prístupom na jeho internetovú stránku, je pre tohto poskytovateľa osobným údajom.

Súdny dvor najskôr uviedol, že na to, aby sa určitý údaj mohol kvalifikovať ako „osobný údaj“ v zmysle článku 2 písm. a) smernice 95/46, nie je potrebné, aby sa všetky informácie umožňujúce identifikovať dotknutú osobu nachádzali v rukách jedinej osoby. Skutočnosť, že ďalšie informácie potrebné na identifikáciu používateľa internetovej stránky nemá k dispozícii poskytovateľ online mediálnych služieb, ale poskytovateľ internetového pripojenia tohto používateľa, tak nemôže vylúčiť, že dynamické IP adresy uchovávané poskytovateľom online mediálnych služieb predstavujú pre tohto poskytovateľa osobné údaje v zmysle článku 2 písm. a) smernice 95/46.

V dôsledku toho Súdny dvor konštatoval, že dynamická IP adresa, ktorú poskytovateľ online mediálnych služieb uchováva v súvislosti s tým, že určitá osoba si prehliadala internetovú stránku, ktorú tento poskytovateľ sprístupnil verejnosti, predstavuje pre tohto poskytovateľa osobný údaj v zmysle článku 2 písm. a) smernice 95/46, ak má k dispozícii právne prostriedky, na základe ktorých dokáže identifikovať dotknutú osobu vďaka ďalším informáciám, ktorými disponuje poskytovateľ internetového pripojenia tejto osoby.

Rozsudok z 20. decembra 2017, Nowak (C-434/16, EU:C:2017:994)

Pán Nowak, účtovný praktikant, neuspel na skúške, ktorú organizovala írska komora účtovníkov. Podľa § 4 zákona o ochrane údajov podal žiadosť o prístup, pokiaľ ide o všetky osobné údaje, ktoré sa ho týkajú a ktoré má v držbe komora účtovníkov. Komora účtovníkov pánovi Nowakovi poskytla niektoré dokumenty, ale odmietla mu odovzdať jeho kópiu skúšky z dôvodu, že neobsahuje osobné údaje, ktoré sa ho týkajú, v zmysle zákona o ochrane údajov.

Vzhľadom na to, že ani komisár pre ochranu údajov nevyhovel jeho žiadosti o prístup z tých istých dôvodov, obrátil sa pán Nowak na vnútroštátne súdy. Supreme Court (Najvyšší súd, Írsko) rozhodujúci o odvolaní podanom pánom Nowakom položil Súdnemu dvoru otázku, či sa má článok 2 písm. a) smernice 95/46 vykladať v tom zmysle, že za takých podmienok, o aké išlo vo veci samej, písomné odpovede uchádzača na odbornej skúške a prípadné poznámky skúšajúceho, ktoré sa na ne vzťahujú, predstavujú osobné údaje týkajúce sa uchádzača v zmysle tohto ustanovenia.

V prvom rade Súdny dvor uviedol, že na to, aby sa určitý údaj mohol kvalifikovať ako „osobný údaj“ v zmysle článku 2 písm. a) smernice 95/46, nevyžaduje sa, aby sa všetky informácie umožňujúce identifikovať dotknutú osobu nachádzali v rukách jedinej osoby. Navyše v prípade, keď skúšajúci nepozná identitu uchádzača pri hodnotení jeho odpovedí v rámci skúšky, samotný subjekt, ktorý skúšku organizuje, v tomto prípade komora účtovníkov, disponuje potrebnými informáciami, ktoré mu umožňujú bez ťažkostí alebo pochybností identifikovať tohto uchádzača prostredníctvom jeho identifikačného čísla uvedeného na kópii skúšky alebo na vrchnom liste tejto kópie, a tak mu priradiť jeho odpovede.

V druhom rade Súdny dvor konštatoval, že písomné odpovede uchádzača na odbornej skúške predstavujú informácie, ktoré súvisia s jeho osobou. Obsah týchto odpovedí totiž odzrkadľuje úroveň znalostí a schopností uchádzača v danej oblasti, ako aj prípadne jeho myšlienkové pochody, úsudok a kritické myslenie. Okrem toho cieľom získavania uvedených odpovedí je zhodnotiť odborné schopnosti uchádzača a jeho spôsobilosť vykonávať predmetné povolanie. Navyše použitie týchto informácií, ktorého výsledkom je najmä úspech alebo neúspech uchádzača na predmetnej skúške, môže mať vplyv na jeho práva a záujmy, keďže môže určiť alebo ovplyvniť napríklad jeho šance na prístup k želanému povolaniu alebo zamestnaniu. Konštatovanie, že písomné odpovede uchádzača na odbornej skúške predstavujú informácie, ktoré sa týkajú tohto kandidáta z dôvodu ich obsahu, účelu alebo účinku, platí okrem iného aj vtedy, keď ide o skúšku s otvorenou knihou.

V treťom rade, pokiaľ ide o poznámky skúšajúceho týkajúce sa odpovedí uchádzača, Súdny dvor konštatoval, že tieto poznámky rovnako ako odpovede uchádzača na skúške predstavujú informácie, ktoré sa ho týkajú, keďže odzrkadľujú názor alebo hodnotenie skúšajúceho týkajúce sa individuálneho výkonu uchádzača na skúške, najmä jeho znalostí a schopností v predmetnej oblasti. Cieľom uvedených poznámok je navyše

zdokumentovať hodnotenie skúšajúceho týkajúce sa výkonu uchádzača a tieto poznámky môžu mať na uchádzača vplyv.

V štvrtom rade Súdny dvor rozhodol, že písomné odpovede uchádzača na odbornej skúške a prípadné poznámky skúšajúceho, ktoré sa na ne vzťahujú, možno podrobiť overovaniu, najmä pokiaľ ide o ich presnosť a nevyhnutnosť ich uchovávania v zmysle článku 6 ods. 1 písm. d) a e) smernice 95/46, a možno ich opraviť alebo vymazať na základe článku 12 písm. b) tejto smernice. Priznanie práva na prístup k týmto odpovediam a poznámkam uchádzačovi podľa článku 12 písm. a) tejto smernice slúži na dosiahnutie cieľa tejto smernice spočívajúceho v zabezpečení ochrany práva na súkromný život tohto uchádzača, pokiaľ ide o spracúvanie údajov, ktoré sa ho týkajú, a to nezávisle od otázky, či uvedený uchádzač má alebo nemá také právo na prístup aj podľa vnútroštátnej právnej úpravy uplatniteľnej na skúšku. Súdny dvor však zdôraznil, že práva na prístup a opravu podľa článku 12 písm. a) a b) smernice 95/46 sa nevzťahujú na skúšobné otázky, ktoré samy osebe nepredstavujú osobné údaje uchádzača.

Vzhľadom na tieto skutočnosti Súdny dvor dospel k záveru, že za takých podmienok, o aké išlo vo veci samej, písomné odpovede uchádzača na odbornej skúške a prípadné poznámky skúšajúceho týkajúce sa týchto odpovedí predstavujú osobné údaje v zmysle článku 2 písm. a) smernice 95/46.

3. Pojem „spracovanie osobných údajov“

Rozsudok zo 6. novembra 2003 (veľká komora), Lindqvist (C-101/01, EU:C:2003:596)

Pani Lindqvist, dobrovoľná pracovníčka v zbore evanjelickej cirkvi vo Švédsku, vytvorila na svojom osobnom počítači internetové stránky, pričom na nich uverejnila osobné údaje týkajúce sa viacerých osôb, ktoré rovnako ako ona dobrovoľne pracovali v uvedenom zbore. Pani Lindqvistovej bola uložená povinnosť zaplatiť pokutu z dôvodu, že použila osobné údaje v rámci automatizovaného spracovania bez toho, aby predtým na švédskom Datainspektion (verejnoprávny orgán na ochranu údajov počítačového prenosu) podala písomné vyhlásenie, že údaje previedla bez povolenia do tretích krajín a že spracovala citlivé osobné údaje.

V rámci konania o odvolaní podanom pani Lindqvistovou proti tomuto rozhodnutiu na Göta hovrätt (Odvolací súd, Švédsko), tento súd podal na Súdny dvor návrh na začatie prejudiciálneho konania, aby najmä zistil, či pani Lindqvist pristúpila k „úplne alebo čiastočne automatizovanému spracovaniu osobných údajov“ v zmysle smernice 95/46.

Súdny dvor konštatoval, že operácia, ktorou sa na internetovej stránke odkazuje na rôzne osoby a ktorou sa tieto osoby identifikujú buď prostredníctvom ich mena alebo iným spôsobom, napríklad prostredníctvom ich telefónneho čísla alebo informácií o ich pracovných podmienkach a záľubách, predstavuje „úplne alebo čiastočne

automatizované spracovanie osobných údajov“ v zmysle tejto smernice. Také spracovanie osobných údajov, ktoré sa uskutoční na účely výkonu dobrovoľníckych alebo náboženských činností, nepatrí pod nijakú z výnimiek z pôsobnosti smernice, keďže nespadá ani do kategórie činností, ktorých cieľom je verejná bezpečnosť, ani do kategórie výlučne osobných alebo domácich činností, ktoré nepatria do pôsobnosti smernice.

Rozsudok z 13. mája 2014 (veľká komora), Google Spain a Google (C-131/12, EU:C:2014:317)

V tomto rozsudku (pozri tiež rubriku II.1. s názvom „Pôsobnosť všeobecnej právnej úpravy“) mal Súdny dvor príležitosť spresniť pojem „spracovanie osobných údajov“ na internete z hľadiska smernice 95/46.

Súdny dvor tak rozhodol, že činnosť vyhľadávača spočívajúca vo vyhľadávaní informácií, ktoré na internete zverejnili alebo umiestnili tretie osoby, v ich automatickom indexovaní, dočasnom uschovaní a napokon v ich sprístupnení používateľom internetu v určitom preferenčnom poradí sa má kvalifikovať ako spracovanie osobných údajov v prípade, že tieto informácie obsahujú osobné údaje. Súdny dvor okrem toho pripomenul, že operácie uvedené v smernici sa musia kvalifikovať ako takéto spracovanie aj vtedy, keď sa týkajú výlučne informácií, ktoré už boli takto uverejnené v médiách. Všeobecná výnimka z uplatnenia smernice by v takomto prípade smernicu zbavila z veľkej časti jej významu.

Rozsudok z 10. júla 2018 (veľká komora), Jehovan todistajat (C-25/17, EU:C:2018:551)

Fínska komisia pre ochranu údajov prijala rozhodnutie, ktorým zakázala náboženskej spoločnosti Jehovovi svedkovia zber alebo spracovanie osobných údajov v súvislosti s podomovou evanjelizačnou činnosťou vykonávanou jej členmi, pokiaľ nebudú splnené podmienky stanovené fínskou právnou úpravou na spracovanie takýchto údajov. Členovia tejto spoločnosti si totiž robia pri svojej podomovej evanjelizačnej činnosti poznámky o stretnutiach s osobami, ktoré ani oni, ani uvedená spoločnosť nepoznajú. Tieto údaje sú zozbierané do záznamu, ktorý slúži na ich vyhľadanie pri prípadnej ďalšej návšteve bez toho, aby o tom boli dotknuté osoby informované a dali k tomu súhlas. V tejto súvislosti spoločnosť Jehovovi svedkovia stanovila pre svojich členov usmernenia o tom, ako si robiť takéto záznamy, pričom tieto usmernenia boli uvedené prinajmenšom v jednom z jej časopisov týkajúcich sa evanjelizačnej činnosti.

Súdny dvor rozhodol, že zber osobných údajov členmi náboženskej spoločnosti v súvislosti s podomovou evanjelizačnou činnosťou a následné spracovanie týchto údajov nespadajú pod výnimky z pôsobnosti smernice 95/46, keďže nepredstavujú ani spracovanie osobných údajov v priebehu činností uvedených v článku 3 ods. 2 prvej zarážke tejto smernice, ani spracovanie osobných údajov fyzickými osobami v priebehu

výlučne osobných alebo domácich činností v zmysle článku 3 ods. 2 druhej zarážky uvedenej smernice.

Rozsudok z 22. júna 2021 (veľká komora), Latvijas Republikas Saeima (Pokutové body) (C-439/19, EU:C:2021:504)

B, fyzickej osobe, boli uložené pokutové body za jeden alebo viacero dopravných priestupkov. Tieto pokutové body zapísala Ceļu satiksmes drošības direkcija (Riaditeľstvo pre bezpečnosť cestnej premávky, Lotyšsko) (ďalej len „CSDD“) do štátneho registra motorových vozidiel a ich vodičov.

Podľa lotyšskej právnej úpravy o cestnej premávke[34] sú informácie o pokutových bodoch uložených vodičom vozidiel zapísané do tohto registra prístupné verejnosti a CSDD ich oznámi každej osobe, ktorá o to požiada, bez toho, aby táto osoba musela preukázať osobitný záujem na získaní týchto informácií, a to aj hospodárskym subjektom na účely opakovaného použitia. Keďže B pochyboval o zákonnosti tejto právnej úpravy, podal ústavnú sťažnosť na Latvijas Republikas Satversmes tiesa (Ústavný súd, Lotyšsko), aby tento súd preskúmal súlad tejto právnej úpravy s právom na rešpektovanie súkromného života.

Ústavný súd dospel k záveru, že v rámci svojho posúdenia tohto ústavného práva musí zohľadniť GDPR. Požiadal teda Súdny dvor, aby objasnil pôsobnosť viacerých ustanovení GDPR s cieľom určiť zlučiteľnosť lotyšskej právnej úpravy o cestnej premávke s týmto nariadením.

Súdny dvor svojím rozsudkom, vyhláseným veľkou komorou, rozhodol, že spracúvanie osobných údajov týkajúcich sa pokutových bodov predstavuje „spracúvanie osobných údajov týkajúcich sa uznania viny za trestné činy a priestupky“,[35] pre ktoré GDPR stanovuje zvýšenú ochranu z dôvodu osobitnej citlivosti predmetných údajov.

V tejto súvislosti na úvod poznamenal, že informácie týkajúce sa pokutových bodov sú osobnými údajmi a že ich oznámenie zo strany CSDD tretím osobám predstavuje spracovanie, ktoré patrí do vecnej pôsobnosti nariadenia GDPR. Táto pôsobnosť je totiž veľmi široká a na toto zaobchádzanie sa nevzťahujú výnimky z uplatniteľnosti tohto nariadenia.

Na jednej strane sa tak na toto spracúvanie nevzťahuje výnimka týkajúca sa neuplatňovania GDPR na spracúvanie vykonávané v rámci činnosti, ktorá nepatrí do pôsobnosti práva Únie.[36] Túto výnimku treba považovať za ustanovenie, ktorého jediným cieľom je vylúčiť z pôsobnosti tohto nariadenia spracúvanie osobných údajov vykonávané štátnymi orgánmi v rámci činnosti, ktorej cieľom je zabezpečiť národnú

[34] Článok 14[1] ods. 2 Ceļu satiksmes likums (zákon o cestnej premávke) z 1. októbra 1997 (Latvijas Vēstnesis, 1997, č. 274/276).
[35] Článok 10 GDPR.
[36] Článok 2 ods. 2 písm. a) GDPR.

bezpečnosť, alebo činnosti, ktorá môže byť zaradená do tej istej kategórie. Tieto činnosti zahŕňajú najmä činnosti, ktorých cieľom je chrániť základné funkcie štátu a základné záujmy spoločnosti. Činnosti týkajúce sa bezpečnosti cestnej premávky však takýto cieľ nesledujú, a teda nemôžu byť zaradené do kategórie činností, ktorých cieľom je ochrana národnej bezpečnosti.

Na druhej strane oznámenie osobných údajov týkajúcich sa pokutových bodov nie je ani spracúvaním, na ktoré sa vzťahuje výnimka stanovujúca neuplatnenie nariadenia GDPR na spracovanie osobných údajov vykonané príslušnými orgánmi v trestných veciach.[37] Súdny dvor totiž konštatuje, že v rámci výkonu uvedeného oznámenia nemožno CSDD považovať za takýto „príslušný orgán".[38]

S cieľom určiť, či prístup k osobným údajom týkajúcim sa dopravných priestupkov, akými sú pokutové body, predstavuje spracovanie osobných údajov týkajúcich sa „trestných činov",[39] na ktoré sa vzťahuje zvýšená ochrana, Súdny dvor konštatuje, pričom sa opiera najmä o genézu nariadenia GDPR, že tento pojem odkazuje výlučne na trestne stíhateľné skutky. Skutočnosť, že v lotyšskom právnom systéme sú dopravné priestupky kvalifikované ako správne delikty, však nie je rozhodujúca na posúdenie, či tieto delikty spadajú pod pojem „trestne stíhateľný skutok", keďže ide o autonómny pojem práva Únie, ktorý v celej Únii vyžaduje autonómny a jednotný výklad. Súdny dvor teda po tom, čo pripomenul tri kritériá relevantné na posúdenie trestnej povahy porušenia, a to právnu kvalifikáciu porušenia vo vnútroštátnom práve, povahu porušenia a stupeň prísnosti uloženej sankcie, rozhodol, že na predmetné dopravné priestupky sa vzťahuje pojem „trestný čin" v zmysle GDPR. Pokiaľ ide o prvé dve kritériá, Súdny dvor konštatuje, že aj keď porušenia nie sú vo vnútroštátnom práve kvalifikované ako „trestné činy", takáto povaha môže vyplývať z povahy porušenia, a najmä z represívneho cieľa sledovaného sankciou, ktorá môže byť uložená v dôsledku porušenia. V prejednávanej veci pritom uloženie pokutových bodov za dopravné priestupky, rovnako ako ďalšie sankcie, ktoré môže ich spáchanie mať za následok, sledujú okrem iného takýto represívny cieľ. Pokiaľ ide o tretie kritérium, Súdny dvor poznamenáva, že iba dopravné priestupky určitej závažnosti zahŕňajú pridelenie pokutových bodov, a teda že takéto priestupky môžu viesť k sankciám určitej prísnosti. Navyše uloženie takýchto bodov sa vo všeobecnosti pripája k uloženej sankcii a kumulácia týchto bodov spôsobuje právne následky, ktoré môžu viesť až k zákazu riadenia motorového vozidla.

[37] Článok 2 ods. 2 písm. d) GDPR.

[38] Článok 3 ods. 7 smernice Európskeho parlamentu a Rady (EÚ) 2016/680 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov príslušnými orgánmi na účely predchádzania trestným činom, ich vyšetrovania, odhaľovania alebo stíhania alebo na účely výkonu trestných sankcií a o voľnom pohybe takýchto údajov a o zrušení rámcového rozhodnutia Rady 2008/977/SVV (Ú. v. EÚ L 119, 2016, s. 89).

[39] Článok 10 GDPR.

Rozsudok z 5. decembra 2023 (veľká komora), Nacionalinis visuomenės sveikatos centras (C-683/21, EU:C:2023:949)

V roku 2020 sa litovské orgány s cieľom lepšie zvládnuť pandémiu COVID-19 rozhodli zorganizovať obstaranie mobilnej IT aplikácie. Táto aplikácia mala prispieť k epidemiologickému monitorovaniu umožnením zaznamenávania a monitorovania údajov o osobách, ktoré boli vystavené vírusu COVID-19.

Na tento účel Nacionalinis visuomenės sveikatos centras prie Sveikatos apsaugos ministerijos (Národné centrum verejného zdravotníctva pri ministerstve zdravotníctva, Litva; ďalej len „NVSC“), poverené týmto obstaraním, kontaktovalo spoločnosť UAB „IT sprendimai sėkmei“ (ďalej len „ITSS“), pričom ju požiadalo o vytvorenie takejto mobilnej aplikácie. Následne zamestnanci NVSC zaslali tejto spoločnosti e-maily týkajúce sa najmä otázok, ktoré mali byť uvedené v tejto aplikácii.

V období od apríla do mája 2020 bola mobilná aplikácia vytvorená spoločnosťou ITSS sprístupnená verejnosti. V dôsledku toho ju využilo 3 802 osôb, pričom tieto osoby poskytli rôzne údaje požadované touto aplikáciou, ktoré sa ich týkali. Z dôvodu nedostatku financovania však NVSC spoločnosti ITSS nezadalo žiadnu verejnú zákazku na oficiálne obstaranie tejto mobilnej aplikácie a ukončilo s tým súvisiace konanie.

Medzitým vnútroštátny dozorný orgán začal vyšetrovanie týkajúce sa spracúvania osobných údajov vyplývajúceho z používania tejto aplikácie. Rozhodnutím tohto orgánu prijatým po skončení vyšetrovania boli uložené správne pokuty tak NVSC, ako aj spoločnosti ITSS považovanej za spoločného prevádzkovateľa.

NVSC napadlo toto rozhodnutie na Vilniaus apygardos administracinis teismas (Krajský správny súd Vilnius, Litva). Keďže mal tento súd pochybnosti o výklade viacerých ustanovení GDPR, podal na Súdny dvor návrh na začatie prejudiciálneho konania.

Súdny dvor zasadajúci v zložení veľkej komory vo svojom rozsudku spresnil okrem iného pojem „spracúvanie“. V tejto súvislosti uviedol, že používanie osobných údajov na IT testovanie mobilnej aplikácie predstavuje spracúvanie v zmysle GDPR. Inak je to však v prípade, ak takéto údaje boli anonymizované takým spôsobom, že osoba dotknutá týmito údajmi nie je alebo už nie je identifikovateľná, alebo ak ide o fiktívne údaje, ktoré sa netýkajú existujúcej fyzickej osoby.

Na jednej strane totiž otázka, či sa osobné údaje používajú na IT testovanie alebo na iný účel, nemá vplyv na kvalifikáciu operácie ako „spracúvania“. Na druhej strane len spracúvanie, ktoré sa týka osobných údajov, možno kvalifikovať ako „spracúvanie“ v zmysle GDPR. Fiktívne alebo anonymné údaje však nepredstavujú osobné údaje.

4. Pojem „registračný systém osobných údajov“

Rozsudok z 10. júla 2018 (veľká komora), Jehovan todistajat (C-25/17, EU:C:2018:551)

V tomto rozsudku (pozri tiež rubriku II.3. s názvom „Pojem ‚spracovanie osobných údajov‘“) Súdny dvor spresnil pojem „registračný systém“ uvedený v článku 2 písm. c) smernice 95/46.

Súdny dvor tak po tom, čo pripomenul, že táto smernica sa uplatňuje na manuálne spracovanie osobných údajov len vtedy, ak spracúvané údaje tvoria súčasť registračného systému, alebo sú určené na to, aby tvorili súčasť registračného systému, rozhodol, že uvedený pojem zahŕňa súbor osobných údajov zozbieraných v rámci podomovej evanjelizačnej činnosti, ktorý obsahuje mená a adresy, ako aj ďalšie informácie týkajúce sa navštívených osôb, ak sú tieto údaje štruktúrované podľa určených kritérií, ktoré v praxi umožňujú ich jednoduché vyhľadanie na neskoršie použitie. Na to, aby takýto súbor spadal pod tento pojem, nie je potrebné, aby obsahoval špecifické záznamy, registre alebo iné vyhľadávacie systémy.

5. Pojem „prevádzkovateľ spracovania osobných údajov“

Rozsudok z 10. júla 2018 (veľká komora), Jehovan todistajat (C-25/17, EU:C:2018:551)

V tejto veci (pozri tiež rubriky II.3. a II.4., nazvané „Pojem ‚spracovanie osobných údajov‘“ a „Pojem ‚registračný systém osobných údajov‘“) sa Súdny dvor vyslovil k zodpovednosti náboženskej spoločnosti za spracovanie osobných údajov uskutočnené v rámci podomovej evanjelizačnej činnosti, ktorú táto spoločnosť organizuje, koordinuje a podporuje.

Súdny dvor tak usúdil, že povinnosť každej osoby dodržiavať pravidlá práva Únie týkajúce sa ochrany osobných údajov nemožno považovať za zásah do organizačnej autonómie náboženských spoločností. V tejto súvislosti dospel k záveru, že článok 2 písm. d) smernice 95/46 v spojení s článkom 10 ods. 1 Charty sa má vykladať v tom zmysle, že umožňuje považovať náboženskú spoločnosť spoločne s jej členmi vykonávajúcimi evanjelizačnú činnosť za prevádzkovateľa spracovania osobných údajov uskutočneného týmito členmi v súvislosti s ich podomovou evanjelizačnou činnosťou, ktorú táto spoločnosť organizuje, koordinuje a podporuje, pričom nie je potrebné, aby uvedená spoločnosť mala prístup k údajom, alebo sa muselo preukázať, že dala svojim členom písomné usmernenia alebo pokyny v súvislosti s týmto spracovaním.

Rozsudok z 5. júna 2018 (veľká komora), Wirtschaftsakademie Schleswig Holstein (C-210/16, EU:C:2018:388)

Nemecký orgán na ochranu údajov ako dozorný orgán v zmysle článku 28 smernice 95/46 nariadil nemeckej spoločnosti špecializujúcej sa na vzdelávanie a poskytovanie služieb odbornej prípravy prostredníctvom fanúšikovskej stránky umiestnenej na sociálnej sieti Facebook, aby deaktivovala svoju fanúšikovskú stránku. Podľa uvedeného orgánu totiž ani daná spoločnosť, ani spoločnosť Facebook neinformovali návštevníkov fanúšikovskej stránky, že táto stránka zbiera ich osobné údaje pomocou súborov „cookies“ a že daná spoločnosť a Facebook tieto údaje následne spracovávajú.

V tomto kontexte Súdny dvor spresnil pojem „prevádzkovateľ“ spracovania osobných údajov. V tejto súvislosti dospel k záveru, že správca fanúšikovskej stránky umiestnenej na Facebooku, akým bola dotknutá spoločnosť vo veci samej, sa svojím nastavením parametrov (okrem iného podľa svojej cieľovej skupiny, ako aj cieľov riadenia alebo podpory svojich činností) podieľa na určení účelov a prostriedkov spracovania osobných údajov návštevníkov svojej fanúšikovskej stránky. Z tohto dôvodu musí byť podľa Súdneho dvora daný správca považovaný v Únii v zmysle článku 2 písm. d) smernice 95/46 za prevádzkovateľa spolu so spoločnosťou Facebook Ireland (dcérska spoločnosť americkej spoločnosti Facebook v Únii).

Rozsudok z 29. júla 2019, Fashion ID (C-40/17, EU:C:2019:629)

V tejto veci mal Súdny dvor príležitosť rozvinúť pojem „prevádzkovateľ spracovania“ z hľadiska umiestnenia „zásuvného modulu“ na webovú stránku.

V prejednávanej veci Fashion ID, nemecká spoločnosť zaoberajúca sa internetovým predajom módnych odevov, umiestnila na svoju internetovú stránku modul sociálnej siete spoločnosti Facebook „Páči sa mi to“. Zdá sa, že toto umiestnenie malo za následok, že keď si návštevník prezerá internetovú stránku spoločnosti Fashion ID, osobné údaje tohto návštevníka sa prenášajú spoločnosti Facebook Ireland. Je zrejmé, že k tomuto prenosu dochádza bez toho, aby si bol toho uvedený návštevník vedomý, a bez ohľadu na to, či je členom sociálnej siete Facebook alebo či klikol na tlačidlo „Páči sa mi to“ spoločnosti Facebook.

Verbraucherzentrale NRW, nemecké neziskové združenie na ochranu záujmov spotrebiteľov, spoločnosti Fashion ID vytýka, že spoločnosti Facebook Ireland preniesla osobné údaje týkajúce sa návštevníkov jej internetovej stránky jednak bez ich súhlasu a jednak v rozpore s informačnými povinnosťami stanovenými v ustanoveniach týkajúcich sa ochrany osobných údajov. Oberlandesgericht Düsseldorf (Vyšší krajinský súd Düsseldorf, Nemecko), ktorý vo veci rozhodoval, požiadal Súdny dvor o výklad viacerých ustanovení smernice 95/46.

Súdny dvor najskôr konštatoval, že takého správcu internetovej stránky, akým je Fashion ID, možno považovať za prevádzkovateľa v zmysle článku 2 písm. d) smernice 95/46.

Táto zodpovednosť prevádzkovateľa je však obmedzená na operáciu alebo všetky operácie spracovania osobných údajov, pri ktorých skutočne určuje účely a prostriedky, t. j. operácie zberu a prenosu predmetných údajov. Naopak, podľa Súdneho dvora sa na prvý pohľad javí ako vylúčené, že by Fashion ID určovala účely a prostriedky neskorších operácií spracovania osobných údajov, ktoré vykonáva Facebook Ireland po tom, čo sú jej postúpené, takže Fashion ID nemôže byť považovaná za prevádzkovateľa s ohľadom na tieto operácie v zmysle daného článku 2 písm. d)

Okrem toho Súdny dvor zdôraznil, že je nevyhnutné, aby správca internetovej stránky a taký dodávateľ modulu sociálnej siete, akým je Facebook Ireland, sledovali týmito operáciami spracovania legitímny záujem v zmysle článku 7 písm. f) smernice 95/46, aby boli tieto operácie vo vzťahu k nemu odôvodnené.

Napokon Súdny dvor spresnil, že súhlas dotknutej osoby uvedený v článku 2 písm. h) a článku 7 písm. a) smernice 95/46 musí získať správca internetovej stránky len v súvislosti s operáciami spracovania osobných údajov, pri ktorých tento správca určuje účely a prostriedky. V takejto situácii informačná povinnosť stanovená v článku 10 tejto smernice spočíva aj na uvedenom správcovi, pričom informácia, ktorú musí tento správca poskytnúť dotknutej osobe, sa musí týkať len operácie alebo všetkých operácií spracovania osobných údajov, pri ktorých tento správca určuje účely a prostriedky.

Rozsudok z 5. decembra 2023 (veľká komora), Nacionalinis visuomenės sveikatos centras (C-683/21, EU:C:2023:949)

V tejto veci (pozri tiež rubriku II.3. s názvom „Pojem ‚spracovanie osobných údajov‘“) Súdny dvor uviedol, že subjekt, ktorý poveril podnik vývojom mobilnej IT aplikácie a ktorý sa v tejto súvislosti podieľal na určení účelov a prostriedkov spracúvania osobných údajov vykonávaného prostredníctvom tejto aplikácie, sa môže považovať za prevádzkovateľa.[40] Toto konštatovanie nemôže spochybniť skutočnosť, že tento subjekt sám neuskutočnil operácie spracúvania takýchto údajov, výslovne neudelil svoj súhlas s uskutočnením konkrétnych operácií takéhoto spracúvania alebo so sprístupnením uvedenej mobilnej aplikácie verejnosti a túto mobilnú aplikáciu neobstaral, s výnimkou toho, že by pred týmto sprístupnením verejnosti uvedený subjekt výslovne nesúhlasil s týmto sprístupnením a z toho vyplývajúcim spracúvaním osobných údajov.

[40] V zmysle článku 4 bodu 7 GDPR.

6. Pojem „spoločný prevádzkovateľ“

Rozsudok z 5. decembra 2023 (veľká komora), Nacionalinis visuomenės sveikatos centras (C-683/21, EU:C:2023:949)

V tejto veci (pozri tiež rubriky II.3. a II.5., nazvané „Pojem ‚spracovanie osobných údajov‘“ a „Pojem ‚prevádzkovateľ spracovania osobných údajov‘“) Súdny dvor poznamenal, že kvalifikácia dvoch subjektov ako spoločných prevádzkovateľov nepredpokladá existenciu dohody medzi týmito subjektmi o určení účelov a prostriedkov spracúvania predmetných osobných údajov, ani existenciu dohody, ktorá stanovuje podmienky týkajúce sa spoločnej zodpovednosti za spracúvanie. Je pravda, že podľa GDPR[41] musia spoloční prevádzkovatelia formou vzájomnej dohody transparentne určiť svoje príslušné zodpovednosti na účely zabezpečenia dodržiavania požiadaviek tohto nariadenia. Existencia takejto dohody však nepredstavuje predpoklad toho, aby boli dva alebo viaceré subjekty kvalifikované ako „spoloční prevádzkovatelia“, ale povinnosť, ktorú GDPR ukladá spoločným prevádzkovateľom, ak už sú takto kvalifikovaní, na účely zabezpečenia dodržiavania požiadaviek tohto nariadenia, ktoré sú im uložené. Táto kvalifikácia tak vyplýva zo samotnej skutočnosti, že na určení účelov a prostriedkov spracúvania sa podieľali viaceré subjekty.

Pokiaľ ide o spoločné určenie účelov a prostriedkov spracúvania dotknutými subjektmi, Súdny dvor spresnil, že ich účasť na tomto určení môže mať rôzne formy a môže vyplývať tak z ich spoločného rozhodnutia, ako aj z ich zbiehajúcich sa rozhodnutí. V tomto poslednom uvedenom prípade sa však tieto rozhodnutia musia dopĺňať tak, aby každé z nich malo konkrétny účinok na určenie účelov a prostriedkov spracúvania.

7. Podmienky zákonnosti spracovania osobných údajov

Rozsudok zo 16. decembra 2008 (veľká komora), Huber (C-524/06, EU:C:2008:724)

Spolkový úrad pre migráciu a utečencov (Bundesamt für Migration und Flüchtlinge, Nemecko) bol zodpovedný za vedenie centrálneho registra, ktorý zhromažďuje určité osobné údaje týkajúce sa cudzincov, ktorí majú na nemeckom území pobyt dlhší ako tri mesiace. Register sa používal na štatistické účely a pri výkone právomocí policajných, bezpečnostných aj súdnych orgánov v oblasti trestného stíhania a vyšetrovania v súvislosti s konaním, ktoré je trestné alebo ohrozuje verejnú bezpečnosť.

Pán Huber, rakúsky štátny príslušník, sa v roku 1996 usadil v Nemecku, aby tam pracoval ako samostatný poisťovací agent. Vzhľadom na to, že pán Huber sa domnieval, že je

[41] Článok 26 ods. 1 GDPR v spojení s jeho odôvodnením 79.

diskriminovaný spôsobom, akým sa spracovávajú údaje, ktoré sa ho týkajú a ktoré sú uložené v dotknutom registri, pričom takáto databáza neexistuje pre nemeckých štátnych príslušníkov, požiadal o výmaz týchto údajov.

V tomto kontexte sa Oberverwaltungsgericht für das Land Nordrhein-Westfalen (Vyšší správny súd spolkovej krajiny Severné Porýnie-Vestfálsko, Nemecko), ktorý rozhodoval spor, obrátil na Súdny dvor s otázkou, či je spracovanie osobných údajov, ktoré bolo vykonané v dotknutom registri, v súlade s právom Únie.

Súdny dvor najskôr pripomenul, že právo občana Únie na pobyt na území členského štátu, ktorého štátnu príslušnosť nemá, nie je nepodmienečné, ale môže podliehať obmedzeniam. Použitie takéhoto registra na účely podpory úradov poverených uplatňovaním právnej úpravy týkajúcej sa práva na pobyt je tak v zásade v súlade so zákazom diskriminácie na základe štátnej príslušnosti stanoveným v článku 12 ods. 1 ES (teraz článok 18 prvý odsek ZFEÚ). Takýto register však nemôže obsahovať iné informácie ako tie, ktoré sú na tento účel nevyhnutné v zmysle smernice o ochrane osobných údajov.

Pokiaľ ide o pojem „nevyhnutnosť“ spracovania v zmysle článku 7 písm. e) smernice 95/46, Súdny dvor najskôr pripomenul, že ide o autonómny pojem práva Únie, ktorý sa má vykladať tak, aby plne zodpovedal cieľu smernice 95/46, ako je definovaný v jej článku 1 ods. 1. Následne konštatoval, že systém spracovania osobných údajov je v súlade s právom Únie, ak obsahuje výlučne údaje nevyhnutné na uplatnenie tejto právnej úpravy uvedenými orgánmi a ak jeho centralizovaný charakter umožňuje účinnejšie uplatnenie tejto právnej úpravy, pokiaľ ide o právo občanov Únie, ktorí nie sú štátnymi príslušníkmi tohto členského štátu, na pobyt.

Za nevyhnutné v zmysle článku 7 písm. e) smernice 95/46 nemožno v nijakom prípade považovať uchovávanie a spracúvanie nominálnych osobných údajov v rámci takéhoto registra na štatistické účely.

Navyše, pokiaľ ide o otázku používania údajov nachádzajúcich sa v registri na účely boja proti trestnej činnosti, Súdny dvor najmä uviedol, že tento cieľ sa týka stíhania spáchaných trestných činov a priestupkov bez ohľadu na štátnu príslušnosť ich páchateľov. Pre členský štát teda v súvislosti s bojom proti trestnej činnosti nemôže byť situácia jeho štátnych príslušníkov iná ako situácia občanov Únie, ktorí nie sú štátnymi príslušníkmi tohto členského štátu a majú pobyt na jeho území. Preto rozdiel v zaobchádzaní medzi týmito štátnymi príslušníkmi a občanmi Únie vyplývajúci zo systematického spracovávania osobných údajov týkajúcich sa len občanov Únie, ktorí nie sú štátnymi príslušníkmi dotknutého členského štátu, s cieľom boja proti trestnej činnosti predstavuje diskrimináciu zakázanú článkom 12 ods. 1 ES.

Rozsudok z 19. októbra 2016, Breyer (C-582/14, EU:C:2016:779)

V tomto rozsudku (pozri tiež rubriku II.2., nazvanú „Pojem ‚osobné údaje'") sa Súdny dvor tiež vyjadril k tomu, či článok 7 písm. f) smernice 95/46 bráni vnútroštátnemu právnemu predpisu, podľa ktorého poskytovateľ online mediálnych služieb môže zhromažďovať a používať osobné údaje používateľa bez jeho súhlasu len v rozsahu nevyhnutnom na umožnenie využitia online média príslušným používateľom a na jeho zúčtovanie a podľa ktorého účel zabezpečenia celkovej funkčnosti online média nemôže odôvodniť použitie údajov po skončení príslušnej operácie prehliadania.

Súdny dvor rozhodol, že článok 7 písm. f) smernice 95/46 bráni dotknutej právnej úprave. Podľa tohto ustanovenia je totiž spracovanie osobných údajov v zmysle tohto ustanovenia zákonné, ak je spracovanie nevyhnutné na účely legitímnych záujmov, ktoré plní kontrolór, alebo tretia strana alebo strany, ktorým sú údaje odhalené, s výnimkou prípadu, keď sú takéto záujmy prevýšené záujmami týkajúcimi sa základných práv a slobôd dotknutej osoby. V tomto prípade však nemecká právna úprava kategoricky a všeobecne vylúčila možnosť spracovania určitých kategórií osobných údajov bez toho, aby pripustila zváženie protichodných práv a záujmov, o ktoré ide v konkrétnom prípade. Táto právna úprava tak protiprávne obmedzuje pôsobnosť tejto zásady stanovenej v článku 7 písm. f) smernice 95/46 tým, že vylučuje, aby účel zabezpečenia celkovej funkčnosti stránok online mediálnych služieb mohol byť predmetom zváženia so záujmami týkajúcimi sa základných práv a slobôd používateľov.

Rozsudok z 27. septembra 2017, Puškár (C-73/16, EU:C:2017:725)

V spore vo veci samej pán Puškár podal na Najvyšší súd Slovenskej republiky návrh, ktorým sa domáhal, aby bola Finančnému riaditeľstvu, všetkým podriadeným daňovým úradom a Kriminálnemu úradu finančnej správy uložená povinnosť nezapísať jeho meno do zoznamu osôb považovaných finančným riaditeľstvom za tzv. „biele kone", ktorý bol vytvorený týmto úradom v rámci správy daní a ktorého aktualizáciu zabezpečuje toto finančné riaditeľstvo, ako aj Kriminálny úrad finančnej správy (ďalej len „sporný zoznam"). Okrem toho žiadal o odstránenie svojho záznamu z týchto zoznamov a z informačného systému finančnej správy.

Najvyšší súd Slovenskej republiky sa za týchto podmienok obrátil na Súdny dvor najmä s otázkou, či právo na rešpektovanie súkromného a rodinného života, obydlia a komunikácie, ktoré je zakotvené v článku 7, a právo na ochranu osobných údajov, ktoré je zakotvené v článku 8 Charty, možno vykladať v tom zmysle, že členskému štátu neumožňujú vytvárať bez súhlasu dotknutej osoby zoznamy osobných údajov na účely správy daní, t. j. že získanie osobných údajov do dispozičnej sféry orgánu verejnej moci na účely potláčania daňových podvodov je nebezpečné samo osebe.

Súdny dvor usúdil, že článok 7 písm. e) smernice 95/46 nebráni spracovaniu osobných údajov orgánmi členského štátu na účely správy daní a potláčania daňových podvodov,

akým je spracovanie, ku ktorému dochádza vytvorením zoznamu dotknutého vo veci samej, bez súhlasu dotknutých osôb jednak pod podmienkou, že tieto orgány boli vnútroštátnou právnou úpravou poverené úlohami vo verejnom záujme v zmysle tohto ustanovenia, vytvorenie tohto zoznamu a zápis mien dotknutých osôb do uvedeného zoznamu sú skutočne spôsobilé a nevyhnutné na účely uskutočnenia sledovaných cieľov a existujú dostatočné dôvody domnievať sa, že dotknuté osoby sa nachádzajú v uvedenom zozname oprávnene, a jednak že všetky podmienky zákonnosti tohto spracovania osobných údajov uložené smernicou 95/46 sú splnené.

Súdny dvor v tejto súvislosti uviedol, že úlohou vnútroštátneho súdu je overiť, či je vytvorenie sporného zoznamu nevyhnutné na výkon predmetných úloh vo verejnom záujme vo veci samej, najmä s prihliadnutím na presný účel vytvorenia sporného zoznamu, právne účinky, ktorým podliehajú osoby nachádzajúce sa v tomto zozname, a verejnú či neverejnú povahu tohto zoznamu. Navyše vzhľadom na zásadu proporcionality je úlohou vnútroštátneho súdu overiť, či vytvorenie sporného zoznamu a zápis mien dotknutých osôb do tohto zoznamu sú spôsobilé uskutočniť nimi sledované ciele a či neexistujú iné menej obmedzujúce prostriedky na dosiahnutie týchto cieľov.

Okrem toho Súdny dvor konštatoval, že skutočnosť, že určitá osoba je zapísaná v spornom zozname, môže zasiahnuť niektoré z jej práv. Zápis do tohto zoznamu by totiž mohol poškodiť jej povesť a dotknúť sa jej vzťahov s daňovými orgánmi. Tento zápis by rovnako mohol zasiahnuť do prezumpcie neviny tejto osoby, zakotvenej v článku 48 ods. 1 Charty, ako aj do slobody podnikania právnických osôb priradených k fyzickým osobám zapísaným v spornom zozname, stanovenej v článku 16 Charty. V dôsledku toho môže byť takýto zásah primeraný len vtedy, ak existujú dostatočné dôvody na podozrenie, že dotknutá osoba fiktívne vykonáva riadiace funkcie v právnických osobách, s ktorými bola spojená, a tým narúša správu daní a potláčanie daňových podvodov.

Okrem toho Súdny dvor usúdil, že ak existoval dôvod obmedziť podľa článku 13 smernice 95/46 niektoré z práv upravených v článkoch 6 a 10 až 12 tejto smernice, ako je právo na informácie dotknutej osoby, takéto obmedzenie malo byť nevyhnutné na ochranu záujmu spomenutého v odseku 1 tohto článku 13, akým je najmä dôležitý hospodársky a finančný záujem v daňovej oblasti, a malo mať základ v legislatívnych opatreniach.

Rozsudok z 11. novembra 2020, Orange Romania (C-61/19, EU:C:2020:901)

Spoločnosť Orange România SA poskytuje mobilné telekomunikačné služby na rumunskom trhu. Dňa 28. marca 2018 Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP) (Národný orgán dohľadu nad spracúvaním osobných údajov, Rumunsko) uložil tejto spoločnosti pokutu za získavanie a uchovávanie kópií dokladov totožnosti jej zákazníkov bez ich platného súhlasu.

Podľa ANSPDCP v období od 1. do 26. marca 2018 Orange România uzavrela písomné zmluvy o poskytovaní mobilných telekomunikačných služieb, ktoré obsahovali zmluvnú podmienku, podľa ktorej boli zákazníci informovaní a súhlasili so získavaním a uchovávaním kópie ich dokladu totožnosti na účely identifikácie. Políčko týkajúce sa tejto zmluvnej podmienky bolo označené prevádzkovateľom pred podpísaním tejto zmluvy.

V tomto kontexte Tribunalul Bucureşti (Krajský súd Bukurešť, Rumunsko) požiadal Súdny dvor o spresnenie podmienok, za ktorých možno súhlas zákazníkov so spracovaním osobných údajov považovať za platný.

Súdny dvor najskôr pripomenul, že právo Únie[42] stanovuje taxatívny zoznam prípadov, v ktorých možno považovať spracúvanie osobných údajov za zákonné. Najmä súhlas dotknutej osoby musí byť slobodne daný, konkrétny, informovaný a jednoznačný.[43] V tejto súvislosti nemôže byť súhlas platne udelený v prípade mlčania, vopred označeného políčka alebo nečinnosti.

Navyše, ak dotknutá osoba dá súhlas v rámci písomného vyhlásenia, ktoré sa týka aj iných skutočností, toto vyhlásenie musí byť predložené v zrozumiteľnej a ľahko dostupnej forme a musí byť formulované jasne a jednoducho. Na to, aby sa dotknutej osobe zabezpečila skutočná slobodná voľba, zmluvné ustanovenia ju nesmú uviesť do omylu s ohľadom na možnosť uzavrieť zmluvu, aj keď odmietne súhlasiť so spracúvaním jej údajov.

Súdny dvor spresnil, že keďže Orange România je prevádzkovateľom spracovania osobných údajov, musí vedieť preukázať zákonnosť spracúvania týchto údajov, a teda v tomto prípade existenciu platného súhlasu svojich zákazníkov. V tejto súvislosti, keďže sa zdá, že dotknutí zákazníci sami neoznačili políčko týkajúce sa získavania a uchovávania kópií ich dokladu totožnosti, samotná skutočnosť, že toto políčko bolo označené, nemôže preukázať pozitívny prejav súhlasu. Vnútroštátnemu súdu prislúcha, aby vykonal na tento účel potrebné overenia.

Podľa Súdneho dvora vnútroštátnemu súdu tiež prináleží posúdiť, či zmluvné ustanovenia, o ktoré ide vo veci samej, mohli alebo nemohli uviesť dotknutých zákazníkov do omylu, pokiaľ ide o možnosť uzavrieť zmluvu bez ohľadu na to, že odmietli dať súhlas so spracúvaním svojich údajov, pričom v tejto súvislosti chýbali presnejšie informácie. Navyše v prípade odmietnutia zákazníka súhlasiť so spracovaním svojich osobných údajov Súdny dvor uviedol, že Orange România vyžadovala, aby tento zákazník písomne vyhlásil, že nesúhlasí so získavaním ani s uchovávaním kópie svojho dokladu totožnosti. Podľa Súdneho dvora takáto dodatočná požiadavka môže nenáležite ovplyvniť slobodu voľby namietať proti tomuto získavaniu a uchovávaniu. V každom prípade, keďže uvedená spoločnosť má povinnosť preukázať, že jej zákazníci svojím

[42] Článok 7 smernice 95/46 a článok 6 GDPR.
[43] Článok 2 písm. h) smernice 95/46 a článok 4 bod 11 GDPR.

aktívnym správaním vyjadrili svoj súhlas so spracúvaním svojich osobných údajov, táto spoločnosť nemôže od nich vyžadovať, aby svoj nesúhlas vyjadrili aktívnym odmietnutím.

Súdny dvor teda dospel k záveru, že zmluvou o poskytovaní telekomunikačných služieb obsahujúcou zmluvnú podmienku, podľa ktorej bola dotknutá osoba informovaná a súhlasila so získavaním, ako aj uchovávaním kópie jej dokladu totožnosti na účely identifikácie, nemožno preukázať, že táto osoba platne poskytla svoj súhlas s týmto získavaním a následným uchovávaním, ak zaškrtávacie políčko odkazujúce na túto zmluvnú podmienku bolo označené prevádzkovateľom pred podpísaním tejto zmluvy, alebo ak zmluvné ustanovenia tejto zmluvy môžu uviesť dotknutú osobu do omylu s ohľadom na možnosť uzavrieť dotknutú zmluvu, aj keď odmietne súhlasiť so spracúvaním jej údajov, alebo ak slobodná voľba namietať proti tomuto získavaniu a uchovávaniu bola nenáležite ovplyvnená týmto prevádzkovateľom tým, že vyžadoval, aby dotknutá osoba na účely odmietnutia udelenia súhlasu s týmto spracovaním vyplnila dodatočný formulár, v ktorom sa zaznamenalo toto odmietnutie.

Rozsudok z 22. júna 2021 (veľká komora), Latvijas Republikas Saeima (Pokutové body) (C-439/19, EU:C:2021:504)

V tomto rozsudku (pozri tiež rubriku II.3. s názvom „Pojem ‚spracovanie osobných údajov'") Súdny dvor rozhodol, že GDPR bráni právnej úprave, ktorá ukladá Ceļu satiksmes drošības direkcija (Riaditeľstvo pre bezpečnosť cestnej premávky, Lotyšsko) (ďalej len „CSDD") povinnosť sprístupniť verejnosti údaje týkajúce sa pokutových bodov uložených vodičom vozidiel za dopravné priestupky bez toho, aby osoba, ktorá žiada o prístup, musela preukázať osobitný záujem na ich získaní. Konštatuje, že najmä vzhľadom na cieľ zvýšenia bezpečnosti cestnej premávky, na ktorý sa odvoláva lotyšská vláda, nie je preukázaná nevyhnutnosť oznámenia osobných údajov týkajúcich sa pokutových bodov uložených za dopravné priestupky. Okrem toho podľa Súdneho dvora takúto právnu úpravu neodôvodňuje ani právo verejnosti na prístup k úradným dokumentom, ani právo na slobodu informácií.

V tomto kontexte Súdny dvor zdôrazňuje, že zvýšenie bezpečnosti cestnej premávky, ktoré sleduje lotyšská právna úprava, predstavuje cieľ všeobecného záujmu uznaný Úniou, a preto členské štáty môžu kvalifikovať bezpečnosť cestnej premávky ako „úlohu vo verejnom záujme".[44] Potreba lotyšského režimu oznamovať osobné údaje týkajúce sa pokutových bodov na zabezpečenie sledovaného cieľa však nie je preukázaná. Na jednej strane totiž lotyšský zákonodarca disponuje mnohými spôsobmi ako možno konať, ktoré by mu umožnili dosiahnuť tento cieľ inými prostriedkami, ktoré menej zasahujú do základných práv dotknutých osôb. Na druhej strane treba prihliadať na citlivosť údajov týkajúcich sa pokutových bodov a na skutočnosť, že ich oznámenie verejnosti môže

[44] Podľa článku 6 ods. 1 písm. e) GDPR je spracúvanie osobných údajov zákonné, ak je „nevyhnutné na splnenie úlohy realizovanej vo verejnom záujme…".

predstavovať závažný zásah do práv na rešpektovanie súkromného života a na ochranu osobných údajov, keďže môže vyvolať nesúhlas spoločnosti a spôsobiť stigmatizáciu dotknutej osoby.

Okrem toho sa Súdny dvor domnieva, že vzhľadom na citlivosť týchto údajov a závažnosť tohto zásahu do týchto dvoch základných práv majú tieto práva prednosť tak pred záujmom verejnosti na prístupe k úradným dokumentom, ako je štátny register vozidiel a ich vodičov, ako aj pred právom na slobodu informácií.

Navyše Súdny dvor z rovnakých dôvodov rozhodol, že GDPR tiež bráni lotyšskej právnej úprave v rozsahu, v akom povoľuje CSDD oznámiť údaje týkajúce sa pokutových bodov uložených vodičom vozidiel za dopravné priestupky hospodárskym subjektom, aby ich tieto subjekty mohli opakovane používať a oznámiť ich verejnosti.

Napokon Súdny dvor spresnil, že zásada prednosti práva Únie bráni tomu, aby vnútroštátny súd, ktorý rozhoduje o ústavnej sťažnosti proti lotyšskej právnej úprave, ktorú Súdny dvor označil za nezlučiteľnú s právom Únie, rozhodol zachovať právne účinky tejto právnej úpravy až do dňa vyhlásenia svojho konečného rozsudku.

III. Spracúvanie osobných údajov v zmysle odvetvovej právnej úpravy

1. Spracúvanie osobných údajov v sektore elektronických komunikácií

Rozsudok z 2. októbra 2018 (veľká komora), Ministerio Fiscal (C-207/16, EU:C:2018:788)

V tejto veci išlo o žiadosť podanú v súvislosti s vyšetrovaním lúpeže peňaženky a mobilného telefónu, ktorú zamietol španielsky vyšetrovací sudca. Konkrétnejšie kriminálna polícia požiadala uvedený súd, aby jej poskytol prístup k identifikačným údajom užívateľov telefónnych čísel aktivovaných z odcudzeného telefónu počas obdobia dvanástich dní odo dňa odcudzenia. Zamietnutie bolo založené na odôvodnení, podľa ktorého zo skutkových okolností trestného stíhania vyplývalo, že nešlo o „závažný“ trestný čin, t. j. podľa španielskeho práva taký, za ktorý bolo možné uložiť trest odňatia slobody na viac ako päť rokov, pričom prístup k identifikačným údajom bol totiž možný len v prípade takéhoto druhu trestného činu.

Súdny dvor po tom, čo pripomenul, že prístup orgánov verejnej moci k osobným údajom uchovávaným poskytovateľmi elektronických komunikačných služieb v rámci trestného vyšetrovania patrí do pôsobnosti smernice 2002/58, rozhodol, že prístup k takým údajom smerujúcim k identifikácii držiteľov SIM kariet aktivovaných s odcudzeným mobilným telefónom, akými sú priezviská, krstné mená a prípadne adresy týchto

držiteľov, predstavuje zásah do základných práv na rešpektovanie súkromného života a ochrany dotknutých údajov, a to aj v prípade neexistencie okolností umožňujúcich posúdiť tento zásah ako „závažný“ a bez toho, aby bolo dôležité, či dotknuté informácie týkajúce sa súkromného života majú alebo nemajú citlivú povahu alebo či pre dotknuté osoby z dôvodu uvedeného zásahu vyplynuli alebo nevyplynuli prípadné nepriaznivé následky. Súdny dvor však zdôraznil, že tento zásah nie je taký závažný, aby v oblasti prevencie, vyšetrovania, odhaľovania a stíhania trestných činov musel byť uvedený prístup obmedzený na boj proti závažnej kriminalite. Hoci smernica 2002/58 taxatívne uvádza ciele, ktorými možno odôvodniť vnútroštátnu právnu úpravu upravujúcu prístup orgánov verejnej moci k dotknutým údajom a odchyľujúcu sa tak od zásady dôvernosti elektronických komunikácií, pričom tento prístup musí skutočne a výlučne zodpovedať jednému z týchto cieľov, Súdny dvor uviedol, že pokiaľ ide o cieľ prevencie, vyšetrovania, odhaľovania a stíhania trestných činov, znenie smernice 2002/58 neobmedzuje tento cieľ iba na boj proti závažným trestným činom, ale vzťahuje sa na „trestné činy“ vo všeobecnosti.

V tejto súvislosti Súdny dvor objasnil, že hoci vo svojom rozsudku Tele2 Sverige a Watson a i.[45] rozhodol, že iba boj proti závažnej kriminalite môže odôvodniť prístup orgánov verejnej moci k osobným údajom uchovávaným poskytovateľmi elektronických komunikačných služieb, ktoré ako celok umožňujú vyvodiť presné závery o súkromnom živote osôb, ktorých údaje sú dotknuté, takýto výklad bol odôvodnený tou skutočnosťou, že cieľ sledovaný právnou úpravou upravujúcou tento prístup musí byť priamo úmerný závažnosti zásahu do dotknutých základných práv, ktorý táto operácia vyvolá. V súlade so zásadou proporcionality tak možno závažný zásah v tejto oblasti odôvodniť iba cieľom boja proti kriminalite, ktorá musí byť tiež považovaná za „závažnú“. Naopak, ak zásah nie je závažný, uvedený prístup môže byť odôvodnený cieľom prevencie, vyšetrovania, odhaľovania a stíhania „trestných činov“ vo všeobecnosti.

Pokiaľ ide o tento prípad, Súdny dvor rozhodol, že prístup výlučne k údajom, ktoré sú predmetom žiadosti dotknutej vo veci samej, nemožno považovať za „závažný“ zásah do základných práv osôb, ktorých údaje sú dotknuté, pretože tieto údaje neumožňujú vyvodiť presné závery týkajúce sa ich súkromného života. Súdny dvor na základe toho dospel k záveru, že zásah, ktorý predstavuje poskytnutie prístupu k takýmto údajom, môže byť teda odôvodnený cieľom prevencie, vyšetrovania, odhaľovania a stíhania „trestných činov“ vo všeobecnosti, bez nutnosti, aby boli tieto trestné činy považované za „závažné“.

[45] Rozsudok z 21. decembra 2016, Tele2 Sverige a Watson a i. (C-203/15 a C-698/15, *EU:C:2016:970*).

Rozsudky zo 6. októbra 2020 (veľká komora), Privacy International (C-623/17, EU:C:2020:790) a La Quadrature du Net a i. (C-511/18, C-512/18 a C-520/18, EU:C:2020:791)

Judikatúra týkajúca sa uchovávania a prístupu k osobným údajom v oblasti elektronických komunikácií, predovšetkým rozsudok Tele2 Sverige a Watson a i., v ktorom Súdny dvor okrem iného rozhodol, že členské štáty nemôžu uložiť poskytovateľom elektronických komunikačných služieb povinnosť vyžadujúcu všeobecné a nediferencované uchovávanie údajov o prenose dát a polohe, znepokojila niektoré štáty, ktoré sa obávali, že ich zbavuje nástroja, ktorý považujú za nevyhnutný na ochranu národnej bezpečnosti a na boj proti trestnej činnosti.

Práve na tomto pozadí začali Investigatory Powers Tribunal (Súd pre kontrolu vyšetrovacích právomocí, Spojené kráľovstvo) (Privacy International, C-623/17), Conseil d'État (Štátna rada, Francúzsko) (La Quadrature du Net a i., spojené veci C-511/18 a C-512/18), ako aj Cour constitutionnelle (Ústavný súd, Belgicko) (Ordre des barreaux francophones et germanophone a i., C-520/18) konať v sporoch týkajúcich sa zákonnosti právnych predpisov, ktoré v týchto oblastiach prijali niektoré členské štáty a ktoré stanovujú najmä povinnosť poskytovateľov elektronických komunikačných služieb odovzdávať orgánom verejnej moci alebo všeobecne a nediferencovane uchovávať údaje používateľov o prenose dát a polohe.

Súdny dvor vo dvoch rozsudkoch vyhlásených vo veľkej komore 6. októbra 2020 najprv rozhodol, že vnútroštátne právne predpisy, ktoré poskytovateľom elektronických komunikačných služieb ukladajú na tento účel povinnosť uchovávať údaje o prenose dát a polohe alebo odovzdávať tieto údaje vnútroštátnym bezpečnostným a spravodajským orgánom, patria do pôsobnosti smernice 2002/58.

Súdny dvor ďalej pripomenul, že smernica 2002/58[46] neumožňuje, aby sa výnimka zo zásadnej povinnosti zabezpečiť dôvernosť elektronických komunikácií a s ňou súvisiacich údajov a zo zákazu uchovávať tieto údaje stala pravidlom. Znamená to, že táto smernica umožňuje členským štátom prijať okrem iného na účely národnej bezpečnosti legislatívne opatrenia na obmedzenie rozsahu práv a povinností stanovených v tejto smernici, a to najmä povinnosti zabezpečiť dôvernosť komunikácie a údajov o prenose dát,[47] pokiaľ sú tieto opatrenia v súlade so všeobecnými zásadami práva Únie, medzi ktoré patrí zásada proporcionality, a so základnými právami zaručenými Chartou[48].

V tejto súvislosti Súdny dvor na jednej strane vo veci Privacy International konštatoval, že smernica 2002/58 v spojení s Chartou bráni vnútroštátnej právnej úprave, ktorá na účely ochrany národnej bezpečnosti ukladá poskytovateľom elektronických komunikačných služieb povinnosť vyžadujúcu všeobecné a nediferencované odovzdávanie údajov o prenose dát a polohe bezpečnostným a spravodajským službám. Na druhej strane

[46] Článok 15 ods. 1 a 3 smernice 2002/58.
[47] Článok 5 ods. 1 smernice 2002/58.
[48] Konkrétne články 7, 8 a 11, ako aj článok 52 ods. 1 Charty.

v spojených veciach La Quadrature du Net a i., ako aj vo veci Ordre des barreaux francophones et germanophone a i. Súdny dvor zastával názor, že tá istá smernica bráni legislatívnym opatreniam, ktoré od poskytovateľov elektronických komunikačných služieb vyžadujú preventívne všeobecné a nediferencované uchovávanie údajov o prenose dát a polohe.

Tieto povinnosti týkajúce sa odovzdávania a všeobecného a nediferencovaného uchovávania takýchto údajov totiž predstavujú obzvlášť závažné zásahy do základných práv zaručených Chartou, pokiaľ správanie osôb nemá spojitosť s cieľom sledovaným predmetnou právnou úpravou. Súdny dvor analogicky podal výklad článku 23 ods. 1 GDPR v spojení s Chartou, a to v tom zmysle, že bráni vnútroštátnej právnej úprave, ktorá ukladá poskytovateľom prístupu verejnosti ku komunikačným službám online a poskytovateľom hostingových služieb povinnosť všeobecne a nediferencovane uchovávať najmä osobné údaje súvisiace s týmito službami.

Naproti tomu Súdny dvor zastával názor, že v situáciách, keď dotknutý členský štát čelí vážnej hrozbe pre národnú bezpečnosť, ktorá sa javí ako skutočná a aktuálna alebo predvídateľná, smernica 2002/58 v spojení s Chartou nebráni možnosti nariadiť poskytovateľom elektronických komunikačných služieb, aby všeobecne a nediferencovane uchovávali údaje o prenose dát a polohe. V tomto kontexte Súdny dvor spresnil, že rozhodnutie, ktorým sa na nevyhnutne potrebnú dobu vydáva takýto príkaz, musí byť podrobené účinnému preskúmaniu zo strany súdu alebo nezávislého správneho orgánu, ktorého rozhodnutie má záväzný účinok, s cieľom overiť existenciu jednej z týchto situácií, ako aj dodržanie stanovených podmienok a záruk. Za tých istých podmienok uvedená smernica nebráni ani automatizovanej analýze údajov, a to najmä údajov o prenose dát a polohe, všetkých používateľov elektronických komunikačných prostriedkov.

Súdny dvor dodal, že smernica 2002/58 v spojení s Chartou nebráni legislatívnym opatreniam, ktoré umožňujú použiť cielené uchovávanie údajov o prenose dát a polohe obmedzené na striktne nevyhnutnú dobu a vymedzené na základe objektívnych a nediskriminačných faktorov, podľa kategórií dotknutých osôb alebo prostredníctvom geografického kritéria. Táto smernica rovnako nebráni takým opatreniam, ktoré stanovujú všeobecné a nediferencované uchovávanie IP adries pridelených zdroju komunikácie, pokiaľ doba uchovávania netrvá dlhšie, než je striktne nevyhnutné, ani opatreniam, ktoré stanovujú všeobecné a nediferencované uchovávanie údajov týkajúcich sa občianskej totožnosti používateľov elektronických komunikačných prostriedkov, pričom členské štáty nie sú v tomto poslednom uvedenom prípade povinné časovo obmedziť uchovávanie. Uvedená smernica navyše nebráni ani legislatívnemu opatreniu umožňujúcemu použiť urýchlené uchovanie údajov, ktoré majú k dispozícii poskytovatelia služieb, ak nastanú situácie, keď je potrebné uchovať uvedené údaje aj po uplynutí zákonom stanovených lehôt uchovávania na účely objasnenia závažných trestných činov alebo narušení v oblasti národnej bezpečnosti, pokiaľ už boli tieto trestné činy alebo narušenia zistené alebo existuje o nich dôvodné podozrenie.

Okrem toho Súdny dvor rozhodol, že smernica 2002/58 v spojení s Chartou nebráni vnútroštátnej právnej úprave, ktorá od poskytovateľov elektronických komunikačných služieb vyžaduje, aby vykonali zber údajov v reálnom čase, a to predovšetkým údajov o prenose dát a polohe, pokiaľ sa tento zber obmedzí na osoby, v prípade ktorých existuje oprávnený dôvod k podozreniu, že sa určitým spôsobom podieľajú na teroristických aktivitách, a podlieha predchádzajúcemu preskúmaniu zo strany súdu alebo nezávislého správneho orgánu, ktorého rozhodnutie má záväzný účinok, aby sa zabezpečilo, že takýto zber údajov v reálnom čase je povolený iba v medziach toho, čo je prísne nevyhnutné. V naliehavých prípadoch sa musí preskúmanie uskutočniť v krátkom čase.

Súdny dvor sa napokon zaoberal otázkou zachovania časových účinkov vnútroštátnej právnej úpravy, ktorá bola vyhlásená za nezlučiteľnú s právom Únie. V tejto súvislosti rozhodol, že vnútroštátny súd nemôže uplatniť ustanovenie vnútroštátneho práva, ktoré ho oprávňuje obmedziť časové účinky vyhlásenia protiprávnosti, ktoré mu prislúcha urobiť, vo vzťahu k vnútroštátnej právnej úprave ukladajúcej poskytovateľom elektronických komunikačných služieb povinnosť všeobecného a nediferencovaného uchovávania údajov o prenose dát a polohe, o ktorom bolo rozhodnuté, že je nezlučiteľné so smernicou 2002/58 v spojení s Chartou.

Za týchto okolností a s cieľom poskytnúť vnútroštátnemu súdu užitočnú odpoveď Súdny dvor pripomenul, že v rámci trestného konania vedeného proti osobám podozrivým zo závažnej trestnej činnosti sa na prípustnosť a posúdenie dôkazov získaných uchovávaním údajov, ktoré je v rozpore s právom Únie, vzťahuje za súčasného stavu práva Únie len vnútroštátne právo. Súdny dvor však spresňuje, že smernica 2002/58 vykladaná z hľadiska zásady efektivity vyžaduje, aby vnútroštátny trestný súd v rámci takého trestného konania vylúčil dôkazy získané prostredníctvom všeobecného a nediferencovaného uchovávania údajov o prenose dát a polohe, ktoré je nezlučiteľné s právom Únie, ak osoby podozrivé zo spáchania trestných činov nie sú schopné účinne sa k týmto dôkazom vyjadriť.

Rozsudok z 2. marca 2021 (veľká komora), Prokuratuur (Podmienky prístupu k údajom týkajúcim sa elektronických komunikácií) (C-746/18, EU:C:2021:152)

Proti H. K. bolo v Estónsku začaté trestné konanie v súvislosti s trestnými činmi krádeže, použitia bankomatovej karty tretej osoby a násilia voči účastníkom súdneho konania. Súd prvého stupňa odsúdil H. K. za tieto trestné činy na trest odňatia slobody na dva roky. Toto rozhodnutie bolo následne potvrdené v odvolacom konaní. Zápisnice, z ktorých vychádza konštatovanie o spáchaní týchto trestných činov, boli vyhotovené predovšetkým na základe osobných údajov získaných v rámci poskytovania elektronických komunikačných služieb. Riigikohus (Najvyšší súd, Estónsko), na ktorý

H.K. podala kasačný opravný prostriedok, vyjadril pochybnosti o tom, či sú podmienky, za ktorých mali vyšetrovacie orgány k týmto údajom prístup, zlučiteľné s právom Únie.[49]

Tieto pochybnosti sa v prvom rade týkajú otázky, či trvanie obdobia, za ktoré mali vyšetrovacie orgány k údajom prístup, predstavuje kritérium umožňujúce posúdiť závažnosť zásahu, ktorý tento prístup predstavuje, do základných práv dotknutých osôb. Ak je toto obdobie veľmi krátke alebo množstvo zhromaždených údajov je veľmi obmedzené, vnútroštátny súd položil otázku, či cieľ boja proti trestnej činnosti vo všeobecnosti, a nielen boja proti závažnej trestnej činnosti, môže takýto zásah odôvodniť. V druhom rade mal vnútroštátny súd pochybnosti, pokiaľ ide o možnosť považovať estónsku prokuratúru, vzhľadom na rôzne úlohy, ktoré jej zveruje vnútroštátna právna úprava, za „nezávislý“ správny orgán v zmysle rozsudku Tele2 Sverige a Watson a i.[50], ktorý môže vyšetrovaciemu orgánu povoliť prístup k dotknutým údajom.

Veľká komora Súdneho dvora vo svojom rozsudku rozhodla, že smernica 2002/58 v spojení s Chartou bráni vnútroštátnej právnej úprave, ktorá umožňuje prístup orgánov verejnej moci k údajom o prenose dát a polohe, ktoré môžu poskytnúť informácie o komunikáciách uskutočnených užívateľom prostriedku elektronickej komunikácie alebo o polohe koncových zariadení, ktoré používa a ktoré umožňujú vyvodiť presné závery o jeho súkromnom živote na účely predchádzania, vyšetrovania, odhaľovania a stíhania trestných činov bez toho, aby sa takýto prístup obmedzoval na konania týkajúce sa boja proti závažnej trestnej činnosti alebo predchádzania vážnym hrozbám pre verejnú bezpečnosť. Dĺžka obdobia, za ktoré bol prístup k uvedeným údajom vyžiadaný, a množstvo alebo druh dostupných údajov v rámci tohto obdobia sú podľa Súdneho dvora v tejto súvislosti irelevantné. Súdny dvor okrem toho konštatoval, že táto smernica v spojení s Chartou bráni vnútroštátnej právnej úprave, ktorá priznáva právomoc prokuratúre povoliť prístup orgánu verejnej moci k údajom o prenose dát a polohe na účely prípravného trestného konania.

Pokiaľ ide o cieľ predchádzania, vyšetrovania, odhaľovania a stíhania trestných činov, sledovaný právnou úpravou dotknutou vo veci samej, Súdny dvor v súlade so zásadou proporcionality konštatoval, že iba ciele boja proti závažnej trestnej činnosti alebo predchádzania závažným hrozbám pre verejnú bezpečnosť môžu odôvodniť prístup orgánov verejnej moci ku všetkým údajom o prenose dát a polohe, ktoré umožňujú vyvodiť presné závery o súkromnom živote dotknutých osôb, pričom iné faktory týkajúce sa proporcionality žiadosti o prístup, ako napríklad dĺžka obdobia, za ktoré sa o prístup k takýmto údajom žiada, nemôžu viesť k tomu, že by cieľ predchádzania, vyšetrovania, odhaľovania a stíhania trestných činov vo všeobecnosti mohol takýto prístup odôvodniť.

Pokiaľ ide o právomoc prokuratúry povoliť prístup orgánu verejnej moci k údajom o prenose dát a polohe na účely prípravného trestného konania, Súdny dvor

[49] Konkrétnejšie s článkom 15 ods. 1 smernice 2002/58 v spojení s článkami 7, 8 a 11, ako aj článkom 52 ods. 1 Charty.
[50] Rozsudok z 21. decembra 2016, Tele2 Sverige a Watson a i. (C-203/15 a C-698/15, *EU:C:2016:970*, bod 120).

pripomenul, že vnútroštátnemu právu prináleží určiť podmienky, za ktorých musia poskytovatelia elektronických komunikačných služieb povoliť príslušným vnútroštátnym orgánom prístup k údajom, ktoré majú k dispozícii. Na účely splnenia požiadavky proporcionality však musí taká právna úprava stanoviť jasné a presné pravidlá, ktoré budú upravovať rozsah a uplatnenie dotknutého opatrenia a ukladať minimálne požiadavky tak, aby osoby, ktorých osobné údaje sú dotknuté, mali dostatočné záruky umožňujúce účinne chrániť tieto údaje pred rizikami zneužitia. Táto právna úprava musí byť podľa vnútroštátneho práva právne záväzná a musí vymedziť okolnosti a hmotnoprávne a procesnoprávne podmienky, za akých možno prijať opatrenie upravujúce spracovanie takýchto údajov, čím zaručí, aby zásah nešiel nad rámec toho, čo je striktne nevyhnutné.

Podľa Súdneho dvora s cieľom zabezpečiť úplné dodržiavanie týchto podmienok v praxi je nevyhnutné, aby prístup príslušných vnútroštátnych orgánov k uchovávaným údajom podliehal predchádzajúcemu preskúmaniu zo strany súdu alebo nezávislého správneho orgánu a aby rozhodnutie tohto súdu alebo orgánu nasledovalo po odôvodnenej žiadosti týchto orgánov podanej v rámci konania týkajúceho sa predchádzania trestným činom, ich odhaľovania a stíhania. V riadne odôvodnených naliehavých prípadoch sa musí preskúmanie uskutočniť v krátkom čase.

V tejto súvislosti Súdny dvor spresňuje, že predchádzajúce preskúmanie okrem iného vyžaduje, aby súd alebo orgán poverený vykonávaním tohto preskúmania disponoval všetkými právomocami a poskytoval záruky potrebné na zosúladenie rôznych dotknutých záujmov a práv. Pokiaľ ide konkrétnejšie o trestné vyšetrovanie, takéto preskúmanie vyžaduje, aby bol tento súd alebo tento orgán schopný zabezpečiť spravodlivú rovnováhu medzi záujmami súvisiacimi s potrebami vyšetrovania v rámci boja proti trestnej činnosti na jednej strane a základnými právami na rešpektovanie súkromného života a na ochranu osobných údajov osôb, ktorých údaje sú predmetom prístupu, na druhej strane. Ak toto preskúmanie nevykonáva súd, ale nezávislý správny orgán, musí mať postavenie, ktoré mu umožní konať pri výkone svojich úloh objektívne a nestranne a musí byť na tento účel chránený pred akýmkoľvek vonkajším vplyvom.

Podľa názoru Súdneho dvora z toho vyplýva, že požiadavka nezávislosti, ktorú musí splniť orgán poverený vykonávaním predchádzajúceho preskúmania, vyžaduje, aby mal tento orgán postavenie tretej osoby vo vzťahu k orgánu, ktorý žiada o prístup k údajom, tak, aby bol tento prvý orgán schopný vykonávať toto preskúmanie objektívne a nestranne bez akéhokoľvek vonkajšieho vplyvu. Konkrétne v trestnoprávnej oblasti požiadavka nezávislosti znamená, že orgán zodpovedný za toto predchádzajúce preskúmanie jednak nie je zapojený do vedenia dotknutého trestného vyšetrovania a jednak je voči účastníkom trestného konania neutrálny. To pritom nie je prípad prokuratúry, ktorá, tak ako estónska prokuratúra, riadi vyšetrovacie konanie a prípadne podáva obžalobu. Z toho vyplýva, že prokuratúra nie je schopná vykonať vyššie uvedené predchádzajúce preskúmanie.

Rozsudok z 5. apríla 2022 (veľká komora), Commissioner of An Garda Síochána a i. (C-140/20, EU:C:2022:258)

V prejednávanej veci Supreme Court (Najvyšší súd, Írsko) predložil návrh na začatie prejudiciálneho konania v rámci občianskoprávneho konania začatého na návrh osoby odsúdenej na doživotie za vraždu spáchanú v Írsku. Táto osoba spochybnila zlučiteľnosť niektorých ustanovení vnútroštátneho zákona o uchovávaní údajov vytvorených v súvislosti s elektronickými komunikáciami, s právom Únie. Na základe tohto zákona boli údaje o prenose dát a polohe týkajúce sa telefonických hovorov obvineného uchovávané poskytovateľmi elektronických komunikačných služieb a sprístupnené policajným orgánom. Pochybnosti, ktoré vyjadril vnútroštátny súd, sa týkali najmä zlučiteľnosti systému všeobecného a nediferencovaného uchovávania týchto údajov v súvislosti s bojom proti závažnej trestnej činnosti so smernicou 2002/58 v spojení s Chartou.

Vo svojom rozsudku vyhlásenom veľkou komorou Súdny dvor potvrdzuje judikatúru vyplývajúcu z rozsudku La Quadrature du Net a i.[51] a spresňuje jej dosah, pričom pripomína, že všeobecné a nediferencované uchovávanie údajov o prenose dát a polohe týkajúcich sa elektronických komunikácií nie je povolené na účely boja proti závažnej trestnej činnosti a predchádzania vážnym hrozbám pre verejnú bezpečnosť. Potvrdzuje tiež judikatúru vyplývajúcu z rozsudku Prokuratuur (Podmienky prístupu k údajom týkajúcim sa elektronických komunikácií)[52], najmä pokiaľ ide o povinnosť podmieniť prístup príslušných vnútroštátnych orgánov k uvedeným uchovávaným údajom predchádzajúcim preskúmaním buď súdom, alebo správnym orgánom, ktorý je vo vzťahu k príslušníkovi polície nezávislý.

Súdny dvor v prvom rade rozhodol, že smernica 2002/58 v spojení s Chartou bráni legislatívnym opatreniam, ktoré na účely boja proti závažnej trestnej činnosti a predchádzania vážnym hrozbám pre verejnú bezpečnosť preventívne stanovujú všeobecné a nediferencované uchovávanie údajov o prenose dát a polohe. S prihliadnutím jednak na odrádzajúci účinok na výkon základných práv[53], ktorý môže vyplynúť z tohto uchovávania, a jednak na závažnosť zásahu, ktorý spôsobí, by takéto uchovávanie malo byť v systéme vytvorenom touto smernicou výnimkou, a nie pravidlom, aby sa takéto údaje nemohli systematicky a nepretržite uchovávať. Trestnú činnosť, a to ani obzvlášť závažnú, nemožno prirovnať k hrozbe pre národnú bezpečnosť, keďže takéto prirovnanie by mohlo zaviesť kategóriu nachádzajúcu sa na rozhraní národnej bezpečnosti a verejnej bezpečnosti s cieľom uplatniť na verejnú bezpečnosť požiadavky, ktoré sú spojené s národnou bezpečnosťou.

Naopak smernica 2002/58 v spojení s Chartou nebráni legislatívnym opatreniam, ktoré na účely boja proti závažnej trestnej činnosti a predchádzania vážnym hrozbám pre

---

[51] Rozsudok zo 6. októbra 2020, La Quadrature du Net a i. (C-511/18, C-512/18 a C-520/18, EU:C:2020:791).
[52] Rozsudok z 2. marca 2021, Prokuratuur (Podmienky prístupu k údajom týkajúcim sa elektronických komunikácií) (C-746/18, EU:C:2021:152).
[53] Zakotvených v článkoch 7 až 11 Charty.

verejnú bezpečnosť stanovujú cielené uchovávanie údajov o prenose dát a polohe, ktoré je vymedzené na základe objektívnych a nediskriminačných faktorov, podľa kategórií dotknutých osôb alebo prostredníctvom geografického kritéria, na časovo obmedzené obdobie, ktoré je striktne nevyhnutné, s možnosťou jeho predĺženia. Súdny dvor dodal, že takéto opatrenie na uchovávanie zamerané na miesta alebo infraštruktúry pravidelne navštevované veľkým počtom osôb, alebo na strategické miesta, akými sú letiská, stanice, námorné prístavy alebo oblasti platenia mýta, umožňuje príslušným orgánom získať informácie o prítomnosti osôb používajúcich prostriedok elektronickej komunikácie na týchto miestach alebo v týchto zemepisných oblastiach, a vyvodiť z toho – na účely boja proti závažnej trestnej činnosti – závery o ich prítomnosti a činnosti na uvedených miestach alebo v uvedených zemepisných oblastiach. V každom prípade prípadná existencia ťažkostí pri presnej definícii prípadov a podmienok, za ktorých možno vykonávať cielené uchovávanie údajov, nemôže odôvodniť to, aby členské štáty stanovili všeobecné a nediferencované uchovávanie údajov o prenose dát a polohe.

Táto smernica v spojení s Chartou nebráni ani legislatívnym opatreniam, ktoré na tie isté účely stanovujú všeobecné a nediferencované uchovávanie IP adries pridelených zdroju spojenia na časovo obmedzené obdobie, ktoré je striktne nevyhnutné, ako aj údajov týkajúcich sa občianskej totožnosti užívateľov elektronických komunikácií. Pokiaľ ide o tento posledný aspekt, Súdny dvor konkrétnejšie spresňuje, že ani smernica 2002/58, ani nijaký iný akt práva Únie nebránia vnútroštátnej právnej úprave, ktorej predmetom je boj proti závažnej trestnej činnosti a podľa ktorej je získanie prostriedku elektronickej komunikácie, akým je predplatená SIM karta, podmienené overením úradných dokladov preukazujúcich občiansku totožnosť kupujúceho a zaznamenaním informácií, ktoré z toho vyplývajú, predávajúcim, pričom predávajúci má prípadne povinnosť sprístupniť tieto informácie príslušným vnútroštátnym orgánom.

To isté platí pre legislatívne opatrenia, ktoré opäť na účely boja proti závažnej trestnej činnosti a predchádzania vážnym hrozbám pre verejnú bezpečnosť stanovujú možnosť prikázať prostredníctvom rozhodnutia príslušného orgánu, ktoré podlieha účinnému súdnemu preskúmaniu, poskytovateľom elektronických komunikačných služieb, aby urýchlene uchovali („quick freeze“) na potrebný čas údaje o prenose dát a polohe, ktoré majú k dispozícii. Iba boj proti závažnej trestnej činnosti a *a fortiori* ochrana národnej bezpečnosti totiž môžu odôvodniť takéto uchovávanie pod podmienkou, že toto opatrenie, ako aj prístup k uchovávaným údajom neprekračujú rámec toho, čo je striktne nevyhnutné. Súdny dvor pripomenul, že takéto opatrenie na rýchle uchovanie sa môže rozšíriť na údaje o prenose dát a polohe týkajúce sa iných osôb, než sú osoby podozrivé z plánovania alebo spáchania závažného trestného činu alebo narušenia v oblasti národnej bezpečnosti, pokiaľ tieto údaje môžu na základe objektívnych a nediskriminačných faktorov prispieť k objasneniu takéhoto trestného činu alebo narušenia v oblasti národnej bezpečnosti, ako sú napríklad údaje týkajúce sa obete tohto činu, ako aj osôb z jej spoločenského alebo profesijného okolia.

Súdny dvor však ďalej uviedol, že všetky vyššie uvedené legislatívne opatrenia musia prostredníctvom jasných a presných pravidiel zabezpečiť, že uchovávanie dotknutých údajov podlieha dodržiavaniu príslušných hmotnoprávnych a procesných podmienok a že dotknuté osoby majú účinné záruky proti rizikám zneužitia. Jednotlivé opatrenia na uchovávanie údajov o prenose dát a polohe sa môžu podľa voľby vnútroštátneho zákonodarcu a pri dodržaní rámca toho, čo je striktne nevyhnutné, uplatniť spoločne.

Okrem toho Súdny dvor spresňuje, že ak by sa na účely boja proti závažnej trestnej činnosti umožnil prístup k takýmto údajom uchovávaným všeobecným a nediferencovaným spôsobom s cieľom čeliť vážnej hrozbe pre národnú bezpečnosť, bolo by to v rozpore s hierarchiou cieľov všeobecného záujmu, ktoré môžu odôvodniť opatrenie prijaté na základe smernice 2002/58. To by totiž znamenalo, že by sa prístup mohol odôvodniť menej dôležitým cieľom, ako je cieľ, ktorý odôvodňuje uchovávanie, a to ochrana národnej bezpečnosti, čím by hrozilo, že zákaz všeobecného a nediferencovaného uchovávania na účely boja proti závažnej trestnej činnosti bude zbavený akéhokoľvek potrebného účinku.

V druhom rade Súdny dvor rozhodol, že smernica 2002/58 v spojení s Chartou bráni vnútroštátnej právnej úprave, podľa ktorej centralizované spracúvanie žiadostí polície o prístup k údajom uchovávaným poskytovateľmi elektronických komunikačných služieb v súvislosti s vyšetrovaním a stíhaním závažných trestných činov, prináleží príslušníkovi polície, a to aj v prípade, že mu pomáha jednotka zriadená v rámci polície, ktorá má pri výkone svojich úloh určitú mieru autonómie a ktorej rozhodnutia môžu byť následne predmetom súdneho preskúmania. Na jednej strane totiž takýto príslušník polície nespĺňa požiadavky nezávislosti a nestrannosti, ktoré musí spĺňať správny orgán vykonávajúci predchádzajúce preskúmanie žiadostí o prístup k údajom pochádzajúcich od príslušných vnútroštátnych orgánov, keďže vo vzťahu k týmto orgánom nemá postavenie tretej osoby. Na druhej strane hoci rozhodnutie takéhoto policajného príslušníka môže byť predmetom následného súdneho preskúmania, toto preskúmanie nemôže nahradiť nezávislé, a s výnimkou riadne odôvodneného naliehavého prípadu, predchádzajúce preskúmanie.

Napokon v treťom rade Súdny dvor potvrdil svoju judikatúru, podľa ktorej právo Únie bráni tomu, aby vnútroštátny súd obmedzil časové účinky vyhlásenia neplatnosti, ktoré mu prislúcha urobiť podľa vnútroštátneho práva, vo vzťahu k vnútroštátnej právnej úprave, ktorá poskytovateľom elektronických komunikačných služieb ukladá povinnosť všeobecného a nediferencovaného uchovávania údajov o prenose dát a polohe, z dôvodu, že táto právna úprava je nezlučiteľná so smernicou 2002/58. Súdny dvor však pripomenul, že prípustnosť dôkazov získaných prostredníctvom takéhoto uchovávania patrí v súlade so zásadou procesnej autonómie členských štátov do pôsobnosti vnútroštátneho práva za predpokladu, že sú dodržané najmä zásady ekvivalencie a efektivity.

Rozsudok z 20. septembra 2022 (veľká komora), VD a SR (C-339/20 a C-397/20, EU:C:2022:703)

V nadväznosti na vyšetrovanie Úradu pre finančné trhy (AMF, Francúzsko) sa začali trestné konania proti VD a SR, dvom fyzickým osobám obvineným z trestných činov obchodovania s využitím dôverných informácií, navádzania na obchodovanie s využitím dôverných informácií, spolupáchateľstva pri trestnom čine, korupcie a legalizácie príjmov z trestnej činnosti. V rámci tohto vyšetrovania AMF použil osobné údaje pochádzajúce z telefonických hovorov VD a SR, vytvorených na základe francúzskeho Zákonníka pôšt a elektronických komunikácií v súvislosti s poskytovaním elektronických komunikačných služieb.

VD a SR sa v rozsahu, v akom sa ich obvinenie zakladalo na údajoch o prenose dát poskytnutých zo strany AMF, obrátili na Cour d'appel de Paris (Odvolací súd Paríž, Francúzsko) so sťažnosťou, pričom uviedli najmä dôvod založený na porušení článku 15 ods. 1 smernice 2002/58 v spojení s článkami 7, 8 a 11, ako aj článkom 52 ods. 1 Charty. Konkrétnejšie, opierajúc sa o judikatúru vyplývajúcu z rozsudku Tele2 Sverige a Watson a i.[54] VD a SR namietali proti skutočnosti, že AMF pri zhromažďovaní uvedených údajov vychádzal z predmetnej vnútroštátnej úpravy, pretože tieto ustanovenia podľa nich jednak neboli v súlade s právom Únie, keďže stanovovali všeobecné a nediferencované uchovávanie údajov o pripojení, a jednak nestanovovali žiadne obmedzenia právomoci vyšetrovateľov AMF získať prístup k uchovávaným údajom.

Cour d'appel de Paris (Odvolací súd Paríž) dvoma rozsudkami z 20. decembra 2018 a zo 7. marca 2019 zamietol sťažnosti VD a SR. Na účely zamietnutia vyššie uvedeného dôvodu sa súdy rozhodujúce vo veciach samých opierali najmä o skutočnosť, že nariadenie o zneužívaní trhu[55] umožňuje príslušným orgánom v rozsahu, v akom to vnútroštátne právo povoľuje, ponechať existujúce záznamy o prenose dát, ktoré majú prevádzkovatelia elektronických komunikačných služieb, ak existujú dôvody domnievať sa, že došlo k porušeniu zákazu obchodovania s využitím dôverných informácií, a ak sa takéto záznamy môžu ukázať ako relevantné na účel vyšetrovania týkajúceho sa tohto porušenia.

VD a SR teda podali v týchto veciach kasačný opravný prostriedok na Cour de cassation (Kasačný súd, Francúzsko), vnútroštátny súd, ktorý podal návrh na začatie prejudiciálneho konania.

V tomto kontexte sa tento súd pýta na súlad článku 15 ods. 1 smernice 2002/58 v spojení s Chartou s požiadavkami vyplývajúcimi z článku 12 ods. 2 písm. a) a d) smernice „o zneužívaní trhu"[56] a článku 23 ods. 2 písm. g) a h) nariadenia o zneužívaní trhu. Táto otázka má svoj pôvod v legislatívnych opatreniach, o ktoré ide vo veci samej,

---

54 Rozsudok z 21. decembra 2016, Tele2 Sverige a Watson a i. (C-203/15 a C-698/15, *EU:C:2016:970*).

55 Nariadenie Európskeho parlamentu a Rady (EÚ) č. 596/2014 zo 16. apríla 2014 o zneužívaní trhu (nariadenie o zneužívaní trhu) a o zrušení smernice Európskeho parlamentu a Rady 2003/6/ES a smerníc Komisie 2003/124/ES, 2003/125/ES a 2004/72/ES (Ú. v. EÚ L 173, 2014, s. 1).

56 Smernica Európskeho parlamentu a Rady 2003/6/ES z 28. januára 2003 o obchodovaní s využitím dôverných informácií a o manipulácii s trhom (zneužívanie trhu) (Ú. v. EÚ L 96, 2003, s. 16; Mim. vyd. 06/004, s. 367).

ktoré preventívne stanovujú, aby prevádzkovatelia elektronických komunikačných služieb všeobecne a nediferencovane uchovávali údaje o prenose dát počas jedného roka odo dňa ich zaznamenania na účely boja proti trestným činom spočívajúcim v zneužívaní trhu, medzi ktoré patrí obchodovanie s využitím dôverných informácií. V prípade, že by Súdny dvor dospel k záveru, že právna úprava týkajúca sa uchovávania údajov o pripojení, o ktorú ide vo veci samej, nie je v súlade s právom Únie, vnútroštátny súd kladie otázku dočasného zachovania účinkov tejto právnej úpravy s cieľom vyhnúť sa právnej neistote a umožniť, aby sa predtým zhromaždené a uchovávané údaje použili na odhaľovanie a stíhanie obchodovania s využitím dôverných informácií.

Súdny dvor zasadajúci vo veľkej komore vo svojom rozsudku rozhodol, že všeobecné a nediferencované uchovávanie údajov o prenose dát počas jedného roka odo dňa ich preventívneho zaznamenania prevádzkovateľmi elektronických komunikačných služieb nie je povolené na účely boja proti trestným činom spočívajúcim v zneužívaní trhu. Okrem toho potvrdzuje svoju judikatúru, podľa ktorej právo Únie bráni tomu, aby vnútroštátny súd časovo obmedzil účinky vyhlásenia neplatnosti, ktoré mu prináleží, pokiaľ ide o ustanovenia vnútroštátnych právnych predpisov, ktoré sú nezlučiteľné s právom Únie.

Súdny dvor v prvom rade pripomenul, že na účely výkladu ustanovenia práva Únie treba zohľadniť nielen jeho znenie, ale aj jeho kontext a ciele sledované právnou úpravou, ktorej je súčasťou, a najmä vývoj tejto právnej úpravy.

Pokiaľ ide o znenie ustanovení uvedených v prejudiciálnych otázkach, Súdny dvor konštatoval, že zatiaľ čo článok 12 ods. 2 písm. d) smernice „o zneužívaní trhu“ odkazuje na právomoc AMF „žiadať existujúce telefónne záznamy a záznamy o prenose údajov“, článok 23 ods. 2 písm. g) a h) nariadenia o zneužívaní trhu odkazuje na právomoc tohto orgánu požadovať jednak „záznamy o prenose údajov, ktoré má k dispozícii investičná spoločnosť, úverová inštitúcia alebo finančná inštitúcia“ a jednak „ak to umožňuje vnútroštátne právo, existujúce záznamy o prenose údajov, ktoré má telekomunikačný operátor“. Podľa Súdneho dvora zo znenia týchto ustanovení jednoznačne vyplýva, že tieto ustanovenia iba vymedzujú právomoc AMF „požadovať“ údaje, ktorými disponujú títo prevádzkovatelia, čo zodpovedá prístupu k týmto údajom. Okrem toho z odkazu na „existujúce“ záznamy ako na „uchovávané“ uvedenými prevádzkovateľmi vyplýva, že normotvorca Únie nemal v úmysle upraviť možnosť vnútroštátneho zákonodarcu zaviesť povinnosť uchovávať takéto záznamy. Podľa Súdneho dvora je tento výklad okrem toho podporený tak kontextom, do ktorého patria uvedené ustanovenia, ako aj cieľmi sledovanými právnou úpravou, ktorej súčasťou sú tieto ustanovenia.

Pokiaľ ide o kontext, do ktorého patria ustanovenia, na ktoré sa vzťahujú prejudiciálne otázky, Súdny dvor poznamenal, že hoci podľa smernice „o zneužívaní trhu“ a nariadenia o zneužívaní trhu,[57] normotvorca Únie mal v úmysle uložiť členským štátom povinnosť

[57] Článok 12 ods. 1 smernice „o zneužívaní trhu“ a článok 23 ods. 3 nariadenia o zneužívaní trhu v spojení s odôvodnením 62 tohto nariadenia.

prijať požadované opatrenia na zabezpečenie toho, aby príslušné finančné orgány mali k dispozícii všetky nástroje, právomoci a zdroje potrebné na to, aby sa tieto informácie poskytli, ako aj právomoci v oblasti dohľadu a vyšetrovania potrebné na zabezpečenie účinného plnenia ich úloh, tieto ustanovenia nehovoria nič o tom, či členské štáty môžu na tieto účely uložiť prevádzkovateľom elektronických komunikačných služieb povinnosť uchovávať údaje o prenose dát všeobecným a nediferencovaným spôsobom, ani o podmienkach, za ktorých musia títo prevádzkovatelia uchovávať takéto údaje na účely ich prípadného odovzdania príslušným orgánom.

Pokiaľ ide o ciele sledované predmetnou právnou úpravou, Súdny dvor uviedol, že zo smernice „o zneužívaní trhu“, ako aj z nariadenia o zneužívaní trhu[58] vyplýva, že tieto nástroje majú za cieľ zabezpečiť integritu finančných trhov Únie a posilniť dôveru investorov v tieto trhy, pričom ide o dôveru, ktorá je založená najmä na skutočnosti, že títo investori majú rovnaké postavenie a sú chránení proti neoprávnenému používaniu dôverných informácií. Zákaz obchodovania s využitím dôverných informácií uvedený v týchto nástrojoch[59] má za cieľ zaručiť rovnosť zmluvných partnerov v burzovej transakcii tým, že sa zabráni tomu, aby jeden z nich, ktorý má dôvernú informáciu a z tohto dôvodu sa ocitol vo výhodnej situácii v porovnaní s ostatnými investormi, z nej ťažil na úkor tých, ktorí o nej nevedia. Hoci podľa nariadenia o zneužívaní trhu[60] záznamy údajov o pripojení predstavujú podstatný a niekedy jediný dôkaz, ktorý umožňuje odhaliť a preukázať existenciu obchodovania s využitím dôverných informácií alebo manipulácie s trhom, nič to nemení na tom, že toto nariadenie sa týka len záznamov, ktoré „majú“ prevádzkovatelia elektronických komunikačných služieb, ako aj právomoci príslušného finančného orgánu „požadovať existujúce“ údaje od týchto prevádzkovateľov. Z tohto znenia teda vôbec nevyplýva, že normotvorca Únie mal ním v úmysle priznať členským štátom právomoc uložiť prevádzkovateľom elektronických komunikačných služieb všeobecnú povinnosť uchovávať údaje. Z toho vyplýva, že ani smernicu „o zneužívaní trhu“, ani nariadenie o zneužívaní trhu nemožno vykladať tak, že by mohli predstavovať právny základ všeobecnej povinnosti uchovávať záznamy o prevádzkových údajoch, ktoré majú prevádzkovatelia elektronických komunikačných služieb, na účely výkonu právomocí udelených príslušnému finančnému orgánu na základe týchto aktov.

Súdny dvor ďalej pripomenul, že smernica 2002/58 predstavuje referenčný akt v oblasti uchovávania a všeobecnejšie spracovania osobných údajov v sektore elektronických komunikácií, takže výklad týkajúci sa tejto smernice sa vzťahuje aj na záznamy prevádzkových údajov, ktoré majú prevádzkovatelia elektronických komunikačných služieb, ktoré môžu príslušné finančné orgány od týchto prevádzkovateľov požadovať v zmysle smernice „o zneužívaní trhu“ a nariadenia o zneužívaní trhu.[61] Posúdenie zákonnosti spracovania záznamov, ktoré majú prevádzkovatelia elektronických

[58] Odôvodnenia 2 a 12 smernice „o zneužívaní trhu“ a článok 1 nariadenia o zneužívaní trhu v spojení s jeho odôvodneniami 2 a 24.
[59] Článok 2 ods. 1 smernice „o zneužívaní trhu“ a článok 8 ods. 1 nariadenia o zneužívaní trhu.
[60] Odôvodnenie 62 nariadenia o zneužívaní trhu.
[61] Článok 11 smernice „o zneužívaní trhu“ a článok 22 nariadenia o zneužívaní trhu.

komunikačných služieb,[62] sa musí uskutočniť so zreteľom na podmienky stanovené v smernici 2002/58, ako aj na výklad tejto smernice obsiahnutý v judikatúre Súdneho dvora.

Súdny dvor tak rozhodol, že smernica „o zneužívaní trhu“ a nariadenie o zneužívaní trhu v spojení so smernicou 2002/58 a s prihliadnutím na Chartu bránia legislatívnym opatreniam, ktoré na preventívne účely stanovujú, aby prevádzkovatelia elektronických komunikačných služieb všeobecne a nediferencovane dočasne uchovávali údaje o prenose dát, teda na jeden rok odo dňa ich zaznamenania, na účely boja proti trestným činom spočívajúcim v zneužívaní trhu, medzi ktoré patrí obchodovanie s využitím dôverných informácií.

Súdny dvor napokon potvrdil svoju judikatúru, podľa ktorej právo Únie bráni tomu, aby vnútroštátny súd obmedzil časové účinky vyhlásenia neplatnosti podľa vnútroštátneho práva vo vzťahu k vnútroštátnym právnym predpisom, ktoré jednak ukladajú prevádzkovateľom elektronických komunikačných služieb povinnosť všeobecného a nediferencovaného uchovávania prevádzkových údajov, a na druhej strane umožňujú poskytnutie takých údajov príslušnému finančnému orgánu bez predchádzajúceho súhlasu súdu alebo nezávislého správneho orgánu, z dôvodu nezlučiteľnosti týchto právnych predpisov so smernicou 2002/58 v spojení s Chartou. Súdny dvor však pripomenul, že prípustnosť dôkazov získaných prostredníctvom takéhoto uchovávania patrí v súlade so zásadou procesnej autonómie členských štátov do pôsobnosti vnútroštátneho práva za predpokladu, že sú dodržané najmä zásady ekvivalencie a efektivity. Táto posledná uvedená zásada vyžaduje, aby vnútroštátny trestný súd v rámci trestného konania vedeného proti osobám podozrivým z trestnej činnosti vylúčil informácie a dôkazy získané prostredníctvom všeobecného a nediferencovaného uchovávania, ktoré je nezlučiteľné s právom Únie, ak dotknuté osoby nie sú schopné účinne sa vyjadriť k týmto informáciám a dôkazom, ktoré pochádzajú z oblasti mimo znalostí súdu a ktoré môžu mať podstatný vplyv na posúdenie skutkového stavu.

Rozsudok z 30. apríla 2024 (plénum), La Quadrature du Net a i. (Osobné údaje a boj proti porušovaniu práv) (C-470/21, EU:C:2024:370)

Na základe návrhu na začatie prejudiciálneho konania, ktorý podala Conseil d'État (Štátna rada, Francúzsko), Súdny dvor, zasadajúci v pléne, rozvinul svoju judikatúru týkajúcu sa smernice 2002/58 tým, že spresnil jednak podmienky, za ktorých sa všeobecné uchovávanie IP adries poskytovateľmi elektronických komunikačných služieb nemusí považovať za také, ktoré spôsobuje závažný zásah do práv na rešpektovanie súkromného života, na ochranu osobných údajov a na slobodu prejavu zaručených Chartou,[63] a jednak možnosť orgánu verejnej moci získať prístup k určitým osobným

[62] V zmysle článku 12 ods. 2 písm. d) smernice „o zneužívaní trhu“ a článku 23 ods. 2 písm. g) a h) nariadenia o zneužívaní trhu.
[63] Články 7, 8 a 11 Charty.

údajom uchovávaným v súlade s takýmito podmienkami v rámci boja proti porušeniam práv duševného vlastníctva, ku ktorým dochádza online.

V prejednávanej veci štyri združenia predložili Premier ministre (predseda vlády, Francúzsko) žiadosť o zrušenie dekrétu o automatizovanom spracúvaní osobných údajov[64]. Vzhľadom na to, že tejto žiadosti sa nevyhovelo, podali tieto združenia na Conseil d'État (Štátna rada) žalobu o neplatnosť tohto implicitného zamietavého rozhodnutia. Podľa ich názoru tento dekrét, ako aj ustanovenia, ktoré tvoria jeho právny základ,[65] porušujú právo Únie.

Podľa francúzskych právnych predpisov má Haute Autorité pour la diffusion des œuvres et la protection des droits sur internet (Vysoký úrad pre šírenie diel a ochranu práv na internete) (Hadopi) na účely identifikácie osôb zodpovedných za porušovanie autorských práv alebo s nimi súvisiacich práv, ku ktorému dochádza online, povolenie na prístup k určitým údajom, ktoré sú povinní uchovávať poskytovatelia elektronických komunikačných služieb. Tieto údaje sa týkajú totožnosti dotknutej osoby zodpovedajúcej jej IP adrese, ktoré predtým zhromaždili organizácie nositeľov práv. Po identifikácii držiteľa IP adresy použitej na činnosti, ktoré predstavujú takéto porušenie, sa Hadopi riadi postupom tzv. „odstupňovanej reakcie". Konkrétne je tento úrad oprávnený zaslať tejto osobe dve odporúčania, ktoré sú podobné upozorneniam, a ak činnosti pretrvávajú, list, v ktorom jej oznámi, že jej činnosti môžu viesť k trestnému stíhaniu. Napokon má právo obrátiť sa na prokuratúru na účely stíhania uvedenej osoby.[66]

V tomto kontexte sa Conseil d'État (Štátna rada) pýta Súdneho dvora na výklad smernice 2002/58 v spojení s Chartou.[67]

V prvom rade, pokiaľ ide o uchovávanie údajov o totožnosti a zodpovedajúcich IP adries, Súdny dvor zdôraznil, že nie každé všeobecné a nediferencované uchovávanie IP adries nevyhnutne predstavuje závažný zásah do práv na rešpektovanie súkromného života, na ochranu osobných údajov a na slobodu prejavu zaručených Chartou.

Povinnosť zabezpečiť takéto uchovávanie môže byť odôvodnená cieľom boja proti trestným činom vo všeobecnosti, ak je skutočne vylúčené, že by toto uchovávanie mohlo viesť k závažným zásahom do súkromného života dotknutej osoby z dôvodu možnosti vyvodiť presné závery o tejto osobe, a to najmä prostredníctvom prepojenia týchto IP adries so súborom údajov o prenose dát alebo polohe.

---

64 Décret nº 2010-236, du 5 mars 2010, relatif au traitement automatisé de données à caractère personnel autorisé par l'article L. 331-29 du code de la propriété intellectuelle dénommé „Système de gestion des mesures pour la protection des œuvres sur internet" (dekrét č. 2010-236 z 5. marca 2010 o automatizovanom spracúvaní osobných údajov povolenom článkom L. 331-29 Zákonníka duševného vlastníctva s názvom „Systém riadenia opatrení na ochranu diel na internete") (JORF č. 56 zo 7. marca 2010, text č.19) v znení décret nº 2017-924, du 6 mai 2017, relatif à la gestion des droits d'auteur et des droits voisins par un organisme de gestion de droits et modifiant le code de la propriété intellectuelle (dekrét č. 2017-924 zo 6. mája 2017 o správe autorských práv a s nimi súvisiacich práv organizáciou správy práv a o zmene Zákonníka duševného vlastníctva (JORF č. 109 z 10. mája 2017, text č. 176).

65 Najmä článok L. 331-21 tretí až piaty odsek Zákonníka duševného vlastníctva.

66 S účinnosťou od 1. januára 2022 sa Hadopi zlúčil s Conseil supérieur de l'audiovisuel (Najvyššia audiovizuálna rada) (CSA), iným nezávislým orgánom verejnej moci, aby vytvorili Autorité de régulation de la communication audiovisuelle et numérique (Úrad pre reguláciu audiovizuálnych a digitálnych komunikácií) (ARCOM). Postup odstupňovanej reakcie však zostal v podstate nezmenený.

67 Článok 15 ods. 1 smernice 2002/58.

Členský štát, ktorý má v úmysle uložiť poskytovateľom elektronických komunikačných služieb takúto povinnosť, sa preto musí ubezpečiť, že spôsoby uchovávania týchto údajov vylučujú, aby bolo možné vyvodiť presné závery o súkromnom živote dotknutých osôb.

Súdny dvor spresnil, že spôsoby uchovávania musia zahŕňať samotnú štruktúru uchovávania, ktorá musí byť v podstate organizovaná tak, aby sa zabezpečilo skutočne nepriepustné oddelenie jednotlivých kategórií uchovávaných údajov. Vnútroštátne pravidlá týkajúce sa týchto spôsobov tak musia zabezpečiť, aby sa každá kategória údajov vrátane údajov o totožnosti a IP adries uchovávala úplne oddelene od ostatných kategórií uchovávaných údajov a aby bolo toto oddelenie skutočne nepriepustné, a to prostredníctvom bezpečného a spoľahlivého informatizovaného systému. Navyše v rozsahu, v akom tieto pravidlá stanovujú možnosť prepojenia uchovávaných IP adries s totožnosťou dotknutej osoby na účely boja proti porušeniam, musia umožniť takéto prepojenie len s použitím účinného technického postupu, ktorý nespochybní efektívnosť nepriepustného oddelenia týchto kategórií údajov. Spoľahlivosť tohto oddelenia musí podliehať pravidelnej kontrole zo strany tretieho orgánu verejnej moci. Pokiaľ uplatniteľné vnútroštátne právne predpisy stanovujú takéto prísne požiadavky, zásah vyplývajúci z tohto uchovávania IP adries nemožno kvalifikovať ako „závažný“.

Súdny dvor preto dospel k záveru, že v prípade legislatívneho rámca, ktorý zaručuje, že žiadna kombinácia údajov neumožní vyvodiť presné závery o súkromnom živote osôb, ktorých údaje sa uchovávajú, smernica 2002/58 v spojení s Chartou nebráni tomu, aby členský štát uložil povinnosť všeobecného a nediferencovaného uchovávania IP adries na obdobie nepresahujúce to, čo je striktne nevyhnutné, na účely boja proti trestným činom vo všeobecnosti.

V druhom rade, pokiaľ ide o prístup k údajom o totožnosti zodpovedajúcim IP adresám, Súdny dvor rozhodol, že smernica 2002/58 v spojení s Chartou v zásade nebráni vnútroštátnej právnej úprave, ktorá orgánu verejnej moci povoľuje prístup k týmto údajom uchovávaným poskytovateľmi elektronických komunikačných služieb oddelene a skutočne nepriepustne, a to s jediným cieľom umožniť tomuto orgánu identifikovať držiteľov týchto adries podozrivých zo zodpovednosti za porušenia autorských práv a s nimi súvisiacich práv na internete, a prijať voči nim opatrenia. V takom prípade musí vnútroštátna právna úprava zakázať zamestnancom, ktorí majú takýto prístup, po prvé sprístupňovať v akejkoľvek forme informácie o obsahu súborov prehliadaných týmito držiteľmi, s výnimkou ich sprístupnenia na účely podania na prokuratúru, po druhé vykonávať akékoľvek sledovanie prechádzania stránok týmito držiteľmi a po tretie používať tieto IP adresy na iné účely, než je prijatie týchto opatrení.

V tomto kontexte Súdny dvor predovšetkým pripomenul, že hoci sloboda prejavu a dôvernosť osobných údajov sú prvoradými záujmami, tieto základné práva nie sú absolútne. V rámci vyváženia dotknutých práv a záujmov musia totiž tieto práva niekedy ustúpiť iným základným právam a požiadavkám všeobecného záujmu, akými sú ochrana verejného poriadku a predchádzanie trestným činom alebo ochrana práv a slobôd iných.

Tak je to najmä v prípade, keď prevaha priznaná uvedeným prvoradým záujmom môže narušiť účinnosť trestného vyšetrovania najmä tým, že znemožňuje alebo nadmerne sťažuje účinnú identifikáciu páchateľa trestného činu a uloženie sankcie voči nemu.

V tom istom kontexte Súdny dvor tiež odkazuje na svoju judikatúru, podľa ktorej, pokiaľ ide o boj proti trestným činom porušujúcim autorské práva alebo s nimi súvisiace práva, ku ktorým dochádza online, okolnosť, že prístup k IP adresám môže predstavovať jediný prostriedok vyšetrovania umožňujúci identifikáciu dotknutej osoby, preukazuje, že uchovávanie týchto adries a prístup k nim sú striktne nevyhnutné na dosiahnutie sledovaného cieľa, a teda zodpovedajú požiadavke proporcionality. Neumožnenie takéhoto prístupu by navyše znamenalo skutočné riziko systémovej beztrestnosti trestných činov spáchaných online alebo ktorých spáchanie alebo prípravu uľahčujú charakteristické znaky internetu. Existencia takéhoto rizika pritom predstavuje relevantnú okolnosť na účely posúdenia v rámci vyvažovania rôznych dotknutých práv a záujmov, či je zásah do práv na rešpektovanie súkromného života, na ochranu osobných údajov a na slobodu prejavu primeraným opatrením vzhľadom na cieľ boja proti trestným činom.

V treťom rade Súdny dvor pri rozhodovaní o tom, či prístup orgánu verejnej moci k údajom o totožnosti zodpovedajúcim IP adrese musí podliehať predchádzajúcemu preskúmaniu zo strany súdu alebo nezávislého správneho orgánu, konštatoval, že požiadavka takéhoto preskúmania sa uplatní vtedy, ak v kontexte vnútroštátnej právnej úpravy predstavuje tento prístup riziko závažného zásahu do základných práv dotknutej osoby v tom zmysle, že by mohol tomuto orgánu verejnej moci umožniť vyvodiť presné závery o súkromnom živote tejto osoby a prípadne vytvoriť jej podrobný profil. Naopak táto požiadavka predchádzajúceho preskúmania sa neuplatní, ak zásah do základných práv nemožno kvalifikovať ako závažný.

V tejto súvislosti Súdny dvor spresnil, že ak je zavedený mechanizmus uchovávania, ktorý zabezpečuje skutočne nepriepustné oddelenie rôznych kategórií uchovávaných údajov, prístup orgánu verejnej moci k údajom o totožnosti zodpovedajúcim IP adresám v zásade nepodlieha požiadavke predchádzajúceho preskúmania. Takýto prístup výlučne na účely identifikácie držiteľa IP adresy totiž vo všeobecnosti nepredstavuje závažný zásah do vyššie uvedených práv.

Súdny dvor však nevylúčil, že v atypických situáciách existuje riziko, že v rámci takého postupu, akým je postup odstupňovanej reakcie dotknutý vo veci samej, môže orgán verejnej moci vyvodiť presné závery o súkromnom živote dotknutej osoby, a to najmä vtedy, ak táto osoba opakovane, či dokonca vo veľkom rozsahu vykonáva činnosti porušujúce autorské práva alebo s nimi súvisiace práva na sieťach so vzájomným sprístupňovaním („peer-to-peer“) v súvislosti s chránenými dielami určitých druhov, ktoré odhaľujú prípadné citlivé informácie o súkromnom živote uvedenej osoby.

V prejednávanej veci držiteľ IP adresy môže byť osobitne vystavený takémuto riziku, ak má orgán verejnej moci rozhodnúť o tom, či postúpi vec prokuratúre na účely jeho

stíhania. S priebehom jednotlivých fáz postupu odstupňovanej reakcie, ktorý je postupným procesom, totiž môže intenzita zásahu do práva na rešpektovanie súkromného života postupne narastať. Prístup príslušného orgánu k súboru údajov týkajúcim sa dotknutej osoby, ktoré boli nazhromaždené v priebehu rôznych etáp tohto postupu, môže umožniť vyvodenie presných záverov o súkromnom živote tejto osoby. V dôsledku toho musí vnútroštátna právna úprava stanoviť predchádzajúce preskúmanie, ku ktorému musí dôjsť skôr, než môže orgán verejnej moci prepojiť údaje o totožnosti s takýmto súborom údajov, a pred prípadným zaslaním listu s oznámením, v ktorom sa konštatuje, že táto osoba sa dopustila skutkov, ktoré môžu byť trestne stíhané. Toto preskúmanie musí okrem toho zachovať účinnosť postupu odstupňovanej reakcie tým, že umožní najmä identifikovať prípady ďalšieho možného opakovania dotknutého protiprávneho konania. Na tento účel musí byť toto konanie organizované a štruktúrované tak, aby údaje o totožnosti osoby zodpovedajúce IP adresám vopred zhromaždeným z internetu nemohli byť osobami zodpovednými za preskúmanie skutkov v rámci príslušného orgánu verejnej moci automaticky prepojené s informáciami, ktoré tento orgán už má k dispozícii a ktoré by mohli umožniť vyvodiť presné závery o súkromnom živote tejto osoby.

Okrem toho, pokiaľ ide o predmet predchádzajúceho preskúmania, Súdny dvor uviedol, že v prípadoch, keď je dotknutá osoba podozrivá z toho, že sa dopustila porušenia, ktoré patrí medzi trestné činy vo všeobecnosti, súd alebo nezávislý správny orgán zodpovedný za toto preskúmanie musí prístup odmietnuť, ak by tento prístup umožnil orgánu verejnej moci vyvodiť presné závery o súkromnom živote uvedenej osoby. Naproti tomu aj prístup umožňujúci vyvodiť takéto presné závery by mal byť povolený v prípadoch, keď je dotknutá osoba podozrivá zo spáchania trestného činu, o ktorom sa dotknutý členský štát môže domnievať, že zasahuje do základného záujmu spoločnosti, a teda patrí medzi závažnú trestnú činnosť.

Súdny dvor tiež spresnil, že predchádzajúce preskúmanie nemôže byť v žiadnom prípade úplne automatizované, pretože pokiaľ ide o trestné vyšetrovanie, takéto preskúmanie vyžaduje vyváženie legitímnych záujmov súvisiacich s bojom proti trestnej činnosti na jednej strane a rešpektovania súkromného života a ochrany osobných údajov na druhej strane. Toto vyváženie si vyžaduje zásah fyzickej osoby, ktorý je o to viac potrebnejší, že automatizácia a veľký rozsah predmetného spracúvania údajov so sebou prináša riziká pre súkromie.

Súdny dvor tak dospel k záveru, že možnosť osôb zodpovedných sa preskúmanie skutkov v rámci orgánu verejnej moci prepojiť údaje o totožnosti osoby zodpovedajúce IP adrese so súbormi, ktoré obsahujú informácie umožňujúce poznať názvy chránených diel, ktorých sprístupnenie na internete odôvodnilo zhromažďovanie IP adries organizáciami nositeľov práv, musí v prípade, keď tá istá osoba zopakovala činnosť porušujúcu autorské právo alebo s ním súvisiace práva, podliehať predchádzajúcemu preskúmaniu zo strany súdu alebo nezávislého správneho orgánu. Toto preskúmanie nemôže byť úplne automatizované a musí k nemu dôjsť pred takýmto prepojením, ktoré

môže v takýchto prípadoch umožniť vyvodenie presných záverov o súkromnom živote uvedenej osoby, ktorej IP adresa bola použitá na činnosti, ktoré môžu porušovať autorské právo alebo s ním súvisiace práva.

V štvrtom a poslednom rade Súdny dvor uviedol, že systém spracúvania údajov používaný orgánom verejnej moci musí podliehať v pravidelných intervaloch kontrole nezávislého orgánu, ktorý má voči tomuto orgánu postavenie tretej strany. Cieľom tejto kontroly je overiť integritu systému vrátane overenia účinných záruk proti rizikám zneužívajúceho alebo nezákonného prístupu k týmto údajom a ich používania, ako aj jeho účinnosti a spoľahlivosti pri odhaľovaní možných porušení.

V tomto rámci Súdny dvor poznamenal, že v prejednávanej veci automatizované spracúvanie osobných údajov vykonávané orgánom verejnej moci na základe informácií týkajúcich sa porušení práv zistených organizáciami nositeľov práv môže zahŕňať určitý počet falošne pozitívnych prípadov a najmä riziko, že potenciálne veľmi veľké množstvo údajov môže byť použité tretími osobami na zneužívajúce alebo protiprávne účely, čo vysvetľuje potrebu takejto kontroly. Súdny dvor okrem toho dodal, že toto spracúvanie musí dodržiavať osobitné pravidlá ochrany týchto údajov stanovené v smernici 2016/680. Hoci totiž v prejednávanej veci nemá orgán verejnej moci vlastné rozhodovacie právomoci v rámci postupu odstupňovanej reakcie, musí byť kvalifikovaný ako „orgán verejnej moci“, ktorý sa podieľa na predchádzaní trestným činom a ich odhaľovaní, a teda patrí do jej pôsobnosti. Osoby zapojené do takéhoto postupu tak musia požívať všetky hmotnoprávne a procesné záruky stanovené smernicou 2016/680, pričom ich stanovenie vo vnútroštátnych právnych predpisoch prináleží overiť vnútroštátnemu súdu.

2. Spracúvanie osobných údajov v trestných veciach

Rozsudok z 12. mája 2021 (veľká komora), Bundesrepublik Deutschland (Červený obežník Interpolu) (C-505/19, **EU:C:2021:376)**

Medzinárodná organizácia kriminálnej polície (ďalej len „Interpol“) vydala v roku 2012 na žiadosť Spojených štátov amerických a na základe zatykača vydaného orgánmi tejto krajiny červený obežník týkajúci sa WS, nemeckého štátneho príslušníka, na účely jeho prípadného vydania. Keď sa v členskom štáte Interpolu zistí miesto pobytu osoby, ktorej sa týka takýto obežník, tento štát je v zásade povinný uskutočniť jej dočasné zadržanie, prípadne monitorovať alebo obmedziť jej pohyb.

Ešte pred vydaním tohto červeného obežníka však bolo proti WS v Nemecku začaté trestné stíhanie, ktoré sa podľa vnútroštátneho súdu týkalo rovnakých skutkov ako tento obežník. Toto konanie bolo právoplatne zastavené v roku 2010 v súlade s osobitným postupom podľa nemeckého práva po tom, čo WS zaplatil určitú peňažnú sumu.

Následne Bundeskriminalamt (Spolkový úrad kriminálnej polície, Nemecko) informoval Interpol, že podľa jeho názoru je z dôvodu tohto skoršieho konania v danom prípade uplatniteľná zásada *ne bis in idem*. Táto zásada zakotvená tak v článku 54 Dohovoru, ktorým sa vykonáva Schengenská dohoda,[68] ako aj v článku 50 Charty, osobitne zakazuje, aby bola osoba, ktorá už bola právoplatne odsúdená alebo oslobodená spod obžaloby, znovu stíhaná za rovnaký trestný čin.

WS podal v roku 2017 na Verwaltungsgericht Wiesbaden (Správny súd Wiesbaden, Nemecko) žalobu proti Nemecku, ktorou sa domáhal toho, aby bola Nemecku uložená povinnosť prijať opatrenia potrebné na odstránenie tohto červeného obežníka. V tejto súvislosti sa WS odvolával okrem porušenia zásady *ne bis in idem* aj na porušenie svojho práva na voľný pohyb zaručeného článkom 21 ZFEÚ, keďže nemohol vstúpiť do zmluvného štátu Schengenskej dohody alebo do členského štátu bez toho, aby mu hrozilo zatknutie. Domnieval sa tiež, že z dôvodu týchto porušení je spracúvanie jeho osobných údajov uvedených v červenom obežníku v rozpore so smernicou 2016/680 o ochrane osobných údajov v trestných veciach.[69]

V tejto súvislosti Verwaltungsgericht Wiesbaden (Správny súd Wiesbaden) rozhodol položiť Súdnemu dvoru otázku týkajúcu sa uplatňovania zásady *ne bis in idem*, a konkrétnejšie možnosti uskutočnenia dočasného zadržania osoby, ktorej sa týka červený obežník, v situácii, o akú ide v tomto prípade. Okrem toho ak je táto zásada uplatniteľná, tento súd sa pýtal, aké to má dôsledky pre spracúvanie osobných údajov uvedených v takomto obežníku zo strany členských štátov.

Vo svojom rozsudku veľkej komory Súdny dvor najmä rozhodol, že ustanovenia smernice 2016/680 v spojení s článkom 54 DVSD a článkom 50 Charty sa majú vykladať v tom zmysle, že nebránia spracúvaniu osobných údajov uvedených v červenom obežníku vydanom Interpolom, pokiaľ nebolo prostredníctvom takéhoto súdneho rozhodnutia preukázané, že na skutky, na ktorých je založený tento obežník, sa uplatňuje zásada *ne bis in idem*, ak takéto spracúvanie spĺňa podmienky stanovené touto smernicou.

Pokiaľ ide o otázku týkajúcu sa osobných údajov uvedených v červenom obežníku Interpolu, Súdny dvor uviedol, že akákoľvek operácia s týmito údajmi, ako je ich zaznamenanie v registroch hľadaných osôb členského štátu, predstavuje „spracúvanie“, na ktoré sa vzťahuje smernica 2016/680.[70] Dospel tiež jednak k záveru, že toto spracúvanie sleduje legitímny účel, a jednak, že ho nemožno považovať za nezákonné len z toho dôvodu, že na skutky, na ktorých je založený červený obežník, by sa mohla

[68] Dohovor, ktorým sa vykonáva Schengenská dohoda zo 14. júna 1985 uzatvorená medzi vládami štátov hospodárskej únie Beneluxu, Nemeckej spolkovej republiky a Francúzskej republiky o postupnom zrušení kontrol na ich spoločných hraniciach (Ú. v. ES L 239, 2000, s. 19; Mim. vyd. 19/002, s. 9) (ďalej len „DVSD“).

[69] Smernica Európskeho parlamentu a Rady (EÚ) 2016/680 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov príslušnými orgánmi na účely predchádzania trestným činom, ich vyšetrovania, odhaľovania alebo stíhania alebo na účely výkonu trestných sankcií a o voľnom pohybe takýchto údajov a o zrušení rámcového rozhodnutia Rady 2008/977/SVV (Ú. v. EÚ L 119, 2016, s. 89).

[70] Pozri článok 2 ods. 1 a článok 3 bod 2 smernice 2016/680.

uplatniť zásada *ne bis in idem*.[71] Takéto spracúvanie orgánmi členských štátov sa môže navyše ukázať ako nevyhnutné práve na účely overenia, či sa uvedená zásada uplatní.

Za týchto podmienok Súdny dvor rozhodol, že smernica 2016/680 v spojení s článkom 54 DVSD a článkom 50 Charty nebráni spracúvaniu osobných údajov uvedených v červenom obežníku, pokiaľ nebolo právoplatným súdnym rozhodnutím preukázané, že v danom prípade sa uplatní zásada *ne bis in idem*. Takéto spracúvanie však musí spĺňať podmienky stanovené touto smernicou. V tomto zmysle musí byť osobitne potrebné na splnenie úlohy realizovanej príslušným vnútroštátnym orgánom na účely predchádzania trestným činom, ich vyšetrovania, odhaľovania alebo stíhania alebo na účely výkonu trestných sankcií.[72]

Na druhej strane ak sa uplatní zásada *ne bis in idem*, zapísanie osobných údajov uvedených v červenom obežníku Interpolu do registrov hľadaných osôb členských štátov už nie je potrebné, keďže dotknutá osoba už nemôže byť za skutky, ktorých sa týka uvedený obežník, trestne stíhaná, a preto za ne nemôže byť ani zatknutá. Z toho vyplýva, že dotknutá osoba musí mať možnosť požiadať o vymazanie týchto údajov. Ak je však tento zápis zachovaný, musí byť sprevádzaný informáciou o tom, že dotknutá osoba už nemôže byť v členskom štáte alebo v zmluvnom štáte stíhaná za rovnaké skutky z dôvodu zásady *ne bis in idem*.

Rozsudok z 21. júna 2022 (veľká komora), Ligue des droits humains (C-817/19, EU:C:2022:491)

V tejto veci (pozri tiež rubriku I.1. s názvom „Súlad sekundárneho práva Únie s právom na ochranu osobných údajov“) Súdny dvor po tom, čo konštatoval platnosť smernice PNR, poskytol objasnenia týkajúce sa výkladu niektorých jej ustanovení[73].

Po prvé uviedol, že smernica vymenúva ciele sledované spracúvaním údajov z PNR taxatívnym spôsobom. Táto smernica preto bráni vnútroštátnej právnej úprave, ktorá povoľuje spracúvanie údajov z PNR na iné účely, než je boj proti teroristickým trestným činom a závažnej trestnej činnosti. Vnútroštátna právna úprava, ktorá navyše pripúšťa ako účel spracúvania údajov z PNR monitorovanie činností, na ktoré sa zameriavajú spravodajské a bezpečnostné služby, môže teda porušovať taxatívnu povahu tohto výpočtu. Podobne systém zriadený smernicou PNR nemožno uplatniť na účely zlepšenia kontroly hraníc a boja proti nelegálnemu prisťahovalectvu. Z toho tiež vyplýva, že údaje z PNR nemožno uchovávať v jednej databáze, do ktorej je možné nahliadať na dosiahnutie týchto, ako aj iných účelov.

Po druhé Súdny dvor objasnil pojem nezávislý vnútroštátny orgán, ktorý je príslušný overiť, či sú splnené podmienky sprístupnenia údajov z PNR na účely ich následného

[71] Pozri článok 4 ods. 1 písm. b) a článok 8 ods. 1 smernice 2016/680.
[72] Pozri článok 1 ods. 1 a článok 8 ods. 1 smernice 2016/680.
[73] Konkrétne článku 2 („Uplatňovanie [smernice] na lety vnútri EÚ“), článku 6 („Spracúvanie údajov PNR“) a článku 12 („Doba uchovávania údajov a depersonalizácia“) smernice PNR.

posúdenia a schváliť takéto sprístupnenie. Konkrétne orgán zriadený ako PIU sa nemôže považovať za takýto orgán, pretože nemá postavenie tretej osoby vo vzťahu k orgánu, ktorý žiada o prístup k údajom. Keďže členmi jeho personálu môžu byť vyslaní zástupcovia orgánov oprávnených požiadať o takýto prístup, PIU sa zdá byť nevyhnutne prepojený s týmito orgánmi. Smernica PNR preto bráni vnútroštátnej právnej úprave, podľa ktorej orgán zriadený ako útvar PIU má tiež postavenie príslušného vnútroštátneho orgánu oprávneného schváliť sprístupnenie údajov z PNR po uplynutí obdobia šiestich mesiacov po prenose týchto údajov PIU.

Po tretie, pokiaľ ide o dobu uchovávania údajov z PNR, Súdny dvor rozhodol, že článok 12 smernice PNR v spojení s článkami 7, 8 a článkom 52 ods. 1 Charty bráni vnútroštátnej právnej úprave, ktorá stanovuje všeobecnú dobu uchovávania týchto údajov v dĺžke piatich rokov, ktorá sa uplatňuje bez rozdielu na všetkých cestujúcich v leteckej doprave.

Podľa Súdneho dvora sa totiž nezdá, že po uplynutí počiatočnej doby uchovávania v dĺžke šiestich mesiacov sa uchovávanie údajov PNR obmedzuje len na to, čo je striktne nevyhnutné, pokiaľ ide o cestujúcich v leteckej doprave, v prípade ktorých ani predbežné posúdenie, ani prípadné overenia vykonané počas počiatočného šesťmesačného obdobia uchovávania, ani žiadna iná okolnosť neodhalili existenciu objektívnych skutočností – ako napríklad skutočnosť, že údaje z PNR dotknutých cestujúcich viedli k pozitívnej zhode overenej v rámci predbežného posúdenia –, ktoré by mohli preukázať riziko v oblasti teroristických trestných činov alebo závažnej trestnej činnosti, ktoré majú prinajmenšom nepriamo objektívnu súvislosť s leteckou cestou týchto cestujúcich. Naproti tomu konštatoval, že uchovávania údajov z PNR všetkých cestujúcich v leteckej doprave, na ktorých sa vzťahuje systém zavedený touto smernicou, počas počiatočnej doby šiestich mesiacov sa v zásade nezdá byť nad rámec toho, čo je striktne nevyhnutné.

Po štvrté Súdny dvor poskytol usmernenia týkajúce sa možného uplatnenia smernice PNR na účely boja proti teroristickým trestným činom a závažnej trestnej činnosti aj na iné druhy prepravy cestujúcich v rámci Únie. Smernica v spojení s článkom 3 ods. 2 ZEÚ, článkom 67 ods. 2 ZFEÚ a článkom 45 Charty pritom bráni systému prenosu a spracovania údajov z PNR pri všetkej doprave uskutočňovanej inými prostriedkami v rámci Únie v prípade neexistencie skutočnej a aktuálnej alebo predvídateľnej teroristickej hrozby, ktorej by čelil dotknutý členský štát. V takejto situácii, rovnako ako pri letoch vnútri EÚ, sa uplatňovanie systému zavedeného smernicou PNR musí obmedziť na údaje z PNR pri doprave, ktorá sa týka najmä určitých spojení alebo schém cestovania či dokonca niektorých staníc alebo námorných prístavov, v súvislosti s ktorými existujú informácie, ktoré môžu odôvodniť takéto uplatňovanie. Je úlohou dotknutého členského štátu, aby určil dopravu, v súvislosti s ktorou existujú takéto informácie, a aby toto uplatňovanie pravidelne prehodnocoval so zreteľom na zmeny podmienok, ktoré odôvodnili jej výber.

IV. Prenos osobných údajov do tretích krajín

Rozsudok zo 6. novembra 2003 (veľká komora), Lindqvist (C-101/01, EU:C:2003:596)

V tejto veci (pozri tiež rubriku II.3. s názvom „Pojem ‚spracovanie osobných údajov'") chcel vnútroštátny súd najmä zistiť, či pani Lindqvist uskutočnila prenos údajov do tretej krajiny v zmysle uvedenej smernice.

Súdny dvor rozhodol, že k „prenosu údajov do tretej krajiny" v zmysle článku 25 smernice 95/46 nedôjde, pokiaľ osoba, ktorá sa nachádza v členskom štáte, vloží osobné údaje na internetovú stránku uloženú u poskytovateľa hostingu usadeného v tom istom alebo v inom členskom štáte, a tieto údaje tak sprístupní každému, kto sa pripojí na internet, a to aj osobám nachádzajúcim sa v tretích krajinách.

Vzhľadom jednak na stav rozvoja internetu v dobe vypracovania smernice 95/46 a jednak na to, že jej kapitola IV, v ktorej sa nachádza uvedený článok 25, neobsahuje kritériá uplatniteľné na používanie internetu, ktorých cieľom by bolo zaručiť dohľad členských štátov nad prenosmi osobných údajov do tretích krajín a zakázať tieto prenosy, ak neposkytujú primeranú úroveň ochrany, nemožno totiž predpokladať, že normotvorca Spoločenstva mal v úmysle do budúcnosti zahrnúť pod pojem „prenos údajov do tretích krajín" takéto uloženie údajov na internetovú stránku, a to aj napriek tomu, že sa tieto údaje takto sprístupnili osobám z tretích krajín, ktoré mali technické prostriedky na získanie prístupu k nim.

Rozsudok zo 6. októbra 2015 (veľká komora), Schrems (C-362/14, EU:C:2015:650)

Pán Schrems, rakúsky občan a používateľ sociálne siete Facebook, predložil Data Protection Commissionner (komisár pre ochranu údajov, Írsko) sťažnosť z dôvodu, že Facebook Ireland zasielala do Spojených štátov osobné údaje svojich používateľov a uchovávala ich na serveroch umiestnených v tejto krajine, kde boli spracovávané. Podľa pána Schremsa právo a prax Spojených štátov neposkytovali dostatočnú ochranu pred sledovaním údajov prenesených do tejto krajiny jej štátnymi orgánmi. Data Protection Commissionner zamietol sťažnosť najmä z dôvodu, že Komisia vo svojom rozhodnutí 2000/520/ES[74] uviedla, že v rámci režimu, nazývaného „bezpečný prístav" (po anglicky „safe harbour")[75], Spojené štáty zaisťujú preneseným osobným údajom primeranú úroveň ochrany.

Práve v tomto kontexte High Court (Vyšší súd, Írsko) požiadal Súdny dvor o výklad článku 25 ods. 6 smernice 95/46/ES, na základe ktorého môže Komisia konštatovať, že

[74] Rozhodnutie Komisie 2000/520/ES z 26. júla 2000 v súlade so smernicou Európskeho parlamentu a Rady 95/46/ES o primeranosti ochrany poskytovanej zásadami „bezpečného prístavu" a súvisiacimi často kladenými otázkami vydanými Ministerstvom obchodu USA (Ú. v. ES L 215, 2000, s. 7; Mim. vyd. 16/001, s. 119).

[75] Systém bezpečného prístavu zahŕňa skupinu zásad týkajúcich sa ochrany osobných údajov, ktoré americké podniky môžu dobrovoľne dodržiavať.

tretia krajina zaisťuje primeranú úroveň ochrany prenesených údajov, ako aj v podstate o to, aby určil platnosť rozhodnutia 2000/520, prijatého Komisiou na základe uvedeného článku 25 ods. 6 smernice 95/46.

Súdny dvor rozhodol, že rozhodnutie Komisie je v celom rozsahu neplatné, pričom predovšetkým zdôraznil, že jeho prijatie vyžaduje riadne odôvodnené konštatovanie zo strany Komisie, že dotknutá tretia krajina skutočne zaisťuje úroveň ochrany základných práv, ktorá je v podstate rovnocenná úrovni ochrany zaručenej v právnom poriadku Únie. Preto v rozsahu, v akom tak Komisia vo svojom rozhodnutí 2000/520/ES neurobila, článok 1 tohto rozhodnutia porušuje požiadavky stanovené v článku 25 ods. 6 smernice 95/46 v spojení s Chartou a je preto neplatný. Zásady bezpečného prístavu sú totiž výlučne uplatniteľné na americké samocertifikované organizácie, ktoré získali osobné údaje z Únie bez toho, aby sa vyžadovalo, že americké orgány verejnej moci budú podliehať týmto zásadám. Navyše rozhodnutie 2000/520 umožňuje zasahovanie do základných práv osôb, ktorých osobné údaje sú alebo by mohli byť prenesené z Únie do Spojených štátov, bez toho, aby obsahovalo ustanovenie týkajúce sa existencie štátnych pravidiel v Spojených štátoch, ktorých cieľom by bolo obmedzenie prípadných zásahov do týchto práv, a ustanovenie o existencii účinnej právnej ochrany pred zásahmi tohto druhu.

Okrem toho Súdny dvor vyhlásil článok 3 rozhodnutia 2000/520 za neplatný v rozsahu, v akom zbavuje vnútroštátne dozorné orgány právomocí, ktoré im vyplývajú z článku 28 smernice 95/46 v prípade, keď osoba uvedie skutočnosti spôsobilé spochybniť zlučiteľnosť rozhodnutia Komisie, ktoré konštatovalo, že tretia krajina zaisťuje primeranú úroveň ochrany, s ochranou súkromného života, slobôd a základných práv osôb. Súdny dvor dospel k záveru, že neplatnosť článkov 1 a 3 rozhodnutia 2000/520 má za následok neplatnosť celého tohto rozhodnutia.

Pokiaľ ide o nemožnosť odôvodniť takýto zásah, Súdny dvor predovšetkým uviedol, že právna úprava Únie obsahujúca zásah do základných práv zaručených článkami 7 a 8 Charty musí stanoviť jasné a presné pravidlá upravujúce rozsah a uplatnenie opatrenia a stanovujúce minimálne požiadavky takým spôsobom, aby osoby, ktorých osobné údaje boli dotknuté, mali dostatočné záruky, ktoré umožnia účinne chrániť ich údaje pred rizikami zneužitia, akýmkoľvek nezákonným prístupom a akýmkoľvek nezákonným použitím. Nevyhnutnosť disponovať takými zárukami je o to dôležitejšia v prípade, keď sú osobné údaje spracovávané automaticky a keď existuje značné riziko nezákonného prístupu k týmto údajom.

Okrem toho treba najmä uviesť, že 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 striktne nevyhnutné. Na striktnú nevyhnutnosť tak nie je obmedzená právna úprava, ktorá všeobecne oprávňuje uchovávanie všetkých osobných údajov každej osoby, ktorej osobné údaje boli prenesené z Únie, bez toho, aby stanovovala akékoľvek rozlíšenie, obmedzenie alebo výnimku na základe sledovaného cieľa, a bez toho, aby sa stanovilo objektívne kritérium

umožňujúce vymedziť prístup orgánov verejnej moci k údajom a ich neskoršie použitie na účely, ktoré sú presné, prísne obmedzené a spôsobilé odôvodniť zásah, ktorý spôsobuje tak prístup, ako aj používanie týchto údajov. Konkrétne právna úprava umožňujúca orgánom verejnej moci všeobecný prístup k obsahu elektronických komunikácií zasahuje do podstaty obsahu základného práva na rešpektovanie súkromného života. Rovnako právna úprava, ktorá neupravuje nijakú možnosť osoby podliehajúcej súdnej právomoci uplatniť právne prostriedky nápravy, aby mala prístup k osobným údajom, ktoré sa jej týkajú, alebo dosiahnuť opravu alebo vymazanie takýchto údajov, nerešpektuje podstatu obsahu základného práva na účinnú súdnu ochranu, ako je upravené článkom 47 Charty.

Stanovisko 1/15 (Dohoda PNR EÚ – Kanada) z 26. júla 2017 (veľká komora) (EU:C:2017:592)

Dňa 26. júla 2017 sa Súdny dvor prvýkrát vyjadril k zlučiteľnosti návrhu medzinárodnej dohody s Chartou, a najmä s ustanoveniami týkajúcimi sa rešpektovania súkromného života, ako aj ochrany osobných údajov.

Európska únia a Kanada dojednali dohodu o prenose a spracovaní údajov z osobného záznamu o cestujúcom (dohoda PNR), ktorá bola podpísaná v roku 2014. Vzhľadom na to, že Rada Európskej únie požiadala Európsky parlament o jej schválenie, Parlament sa rozhodol obrátiť na Súdny dvor s otázkou, či je zamýšľaná dohoda v súlade s právom Únie.

Zamýšľaná dohoda umožňuje systematický a priebežný prenos údajov z PNR, ktoré sa týkajú všetkých cestujúcich v leteckej doprave, kanadskému orgánu na účely ich využívania a uchovávania, ako aj ich prípadného následného prenosu ďalším orgánom a ďalším tretím krajinám, a to s cieľom boja proti terorizmu a závažnej nadnárodnej trestnej činnosti. Na tento účel zamýšľaná dohoda stanovuje najmä päťročné obdobie uchovávania údajov a osobitné požiadavky týkajúce sa bezpečnosti a integrity údajov z PNR, akými je napríklad bezodkladné maskovanie citlivých údajov, a takisto stanovuje právo na prístup k údajom, na ich opravu a výmaz, ako aj možnosť podať správny alebo súdny opravný prostriedok.

Údaje z PNR, na ktoré sa vzťahuje zamýšľaná dohoda, zahŕňajú popri mene cestujúceho alebo cestujúcich v leteckej doprave najmä informácie, ktoré sú nevyhnutné na rezerváciu, ako sú dátumy plánovanej cesty, cestovná trasa, informácie týkajúce sa leteniek, skupiny osôb zaregistrovaných pod rovnakým rezervačným číslom, informácie o spôsobe platby a fakturácii, informácie o batožine, ako aj všeobecné poznámky vo vzťahu k cestujúcim.

Vo svojom stanovisku Súdny dvor rozhodol, že dohodu PNR nemožno uzavrieť v jej súčasnej podobe z dôvodu nezlučiteľnosti viacerých jej ustanovení so základnými právami uznanými Úniou.

Súdny dvor v prvom rade konštatoval, že tak prenos údajov z PNR z Únie príslušnému kanadskému orgánu, ako aj vymedzenie rámca, ktoré dojednala Únia s Kanadou, pokiaľ ide o podmienky týkajúce sa uchovávania týchto údajov, ich využívania, ako aj ich prípadného následného poskytovania iným kanadským orgánom, Europolu, Eurojustu, justičným alebo policajným orgánom členských štátov alebo aj orgánom iných tretích krajín, predstavujú zásahy do práva zaručeného článkom 7 Charty. Tieto operácie tiež predstavujú zásah do základného práva na ochranu osobných údajov zaručeného článkom 8 Charty, pretože sú spracovaním osobných údajov.

Navyše zdôraznil, že aj keď sa v prípade niektorých údajov z PNR, posudzovaných samostatne, nezdá, že by odhaľovali dôležité informácie o súkromnom živote dotknutých osôb, nič to nemení na tom, že uvedené údaje, ak sú posudzované spoločne, môžu okrem iného odhaliť celú cestovnú trasu, cestovné zvyky, vzťahy, ktoré existujú medzi dvomi alebo viacerými osobami, ako aj informácie o finančnej situácii cestujúcich v leteckej doprave, ich stravovacích návykoch alebo o ich zdravotnom stave a mohli by tiež poskytnúť také citlivé informácie o týchto cestujúcich, aké sú vymedzené v článku 2 písm. e) zamýšľanej dohody (informácie, ktoré poukazujú na rasový alebo etnický pôvod, politické názory, vierovyznanie, atď.).

Súdny dvor v tejto súvislosti usúdil, že hoci dotknuté zásahy možno odôvodniť sledovaním cieľa všeobecného záujmu (zaistenie verejnej bezpečnosti v rámci boja proti teroristickým trestným činom a závažnej nadnárodnej trestnej činnosti), viaceré ustanovenia dohody sa neobmedzujú na to, čo je striktne nevyhnutné, a nestanovujú jasné a presné pravidlá.

Súdny dvor konkrétne uviedol, že vzhľadom na riziko, že spracúvanie údajov bude v rozpore so zásadou zákazu diskriminácie, bolo by potrebné, aby bol prenos citlivých údajov do Kanady presne a osobitne dôkladne odôvodnený, a to na základe iných dôvodov, než je ochrana verejnej bezpečnosti pred terorizmom a závažnou nadnárodnou trestnou činnosťou. V tomto prípade však takéto odôvodnenie chýba. Súdny dvor z toho vyvodil, že ustanovenia dohody týkajúce sa prenosu citlivých údajov do Kanady, ako aj ich spracúvania a uchovávania sú nezlučiteľné so základnými právami.

Súdny dvor v druhom rade usúdil, že pokračujúce uchovávanie údajov z PNR v prípade všetkých cestujúcich v leteckej doprave po ich odlete z Kanady, ktoré umožňuje zamýšľaná dohoda, sa neobmedzuje na to, čo je striktne nevyhnutné. Pokiaľ ide o cestujúcich v leteckej doprave, v prípade ktorých nebolo riziko v oblasti terorizmu alebo závažnej nadnárodnej trestnej činnosti identifikované pri ich prílete do Kanady a až do chvíle, kým neopustili túto krajinu, sa totiž nezdá, že by po ich odlete existoval hoci len nepriamy vzťah medzi ich údajmi z PNR a cieľom sledovaným zamýšľanou dohodou, ktorý by odôvodňoval uchovávanie týchto údajov. Naproti tomu uchovávanie údajov z PNR týkajúcich sa cestujúcich v leteckej doprave, v prípade ktorých boli identifikované objektívne skutočnosti, na základe ktorých možno prijať záver, že títo cestujúci by mohli aj po svojom odlete z Kanady predstavovať riziko z hľadiska boja proti

terorizmu a závažnej nadnárodnej trestnej činnosti, je prípustné aj po skončení ich pobytu v tejto krajine, a to aj počas obdobia piatich rokov.

Súdny dvor v treťom rade konštatoval, že so základným právom na rešpektovanie súkromného života, ktoré je zakotvené v článku 7 Charty, je spojená možnosť dotknutej osoby ubezpečiť sa, že jej osobné údaje sa spracovávajú presne a zákonne. Na to, aby táto osoba mohla vykonať potrebné overenia, musí disponovať právom na prístup k svojim údajom, ktoré sa spracovávajú.

V tejto súvislosti zdôraznil, že v zamýšľanej dohode je potrebné, aby cestujúci v leteckej doprave boli informovaní o prenose svojich údajov z osobného záznamu o cestujúcom do tretej krajiny a o využívaní týchto údajov od okamihu, keď týmto sprístupnením nebude možné ohroziť prebiehajúce vyšetrovania vedené štátnymi orgánmi, ktorých sa týka zamýšľaná dohoda. Takáto informácia sa totiž zdá byť skutočne nevyhnutná na to, aby cestujúci v leteckej doprave mohli uplatniť svoje právo žiadať o prístup k údajom, ktoré sa ich týkajú, a prípadne o ich opravu, ako aj podať v súlade s článkom 47 prvým odsekom Charty účinný prostriedok nápravy pred súdom.

V prípadoch, v ktorých nastanú objektívne skutočnosti odôvodňujúce využitie údajov z osobného záznamu o cestujúcom na účely boja proti terorizmu a závažnej nadnárodnej trestnej činnosti a vyžadujúce predchádzajúce povolenie zo strany súdu alebo nezávislého správneho orgánu, sa tak individuálne informovanie cestujúcich v leteckej doprave zdá byť nevyhnutné. To isté platí v prípade, keď sa údaje z osobného záznamu o cestujúcom v leteckej doprave sprístupňujú iným štátnym orgánom alebo jednotlivcom. K takémuto informovaniu však môže dôjsť až v okamihu, keď ním nebude možné ohroziť prebiehajúce vyšetrovania vedené štátnymi orgánmi, ktorých sa týka zamýšľaná dohoda.

***Rozsudok 16. júla 2020 (veľká komora), Facebook Ireland a Schrems (C-311/18*, EU:C:2020:559)**

GDPR stanovuje, že prenos takýchto údajov do tretej krajiny sa môže v zásade uskutočniť iba vtedy, ak dotknutá tretia krajina zaručuje týmto údajom primeranú úroveň ochrany. Podľa tohto nariadenia môže Komisia konštatovať, že tretia krajina zaručuje z titulu jej vnútroštátneho práva alebo medzinárodných záväzkov, ktoré prevzala, primeranú úroveň ochrany.[76] V prípade neexistencie takého rozhodnutia o primeranosti sa takýto prenos môže uskutočniť len vtedy, ak vývozca osobných údajov usadený v Únii poskytne primerané záruky, ktoré môžu vyplývať najmä zo štandardných doložiek o ochrane údajov prijatých Komisiou, a pod podmienkou, že dotknuté osoby majú vymožiteľné práva a účinné právne prostriedky nápravy.[77] Okrem toho GDPR

[76] Článok 45 GDPR.
[77] Článok 46 ods. 1 a článok 46 ods. 2 písm. c) GDPR.

presne stanovuje podmienky, za akých sa takýto prenos môže uskutočniť bez rozhodnutia o primeranosti alebo primeraných záruk.[78]

Maximillian Schrems, rakúsky štátny príslušník s bydliskom v Rakúsku, je používateľom siete Facebook od roku 2008. Rovnako ako v prípade osobných údajov iných používateľov s bydliskom v Únii sú údaje pána Schremsa v celom rozsahu alebo sčasti prenášané spoločnosťou Facebook Ireland na servery patriace spoločnosti Facebook Inc. nachádzajúce sa na území Spojených štátov, kde sa spracúvajú. Pán Schrems predložil írskemu dozornému orgánu sťažnosť, ktorou sa v podstate domáhal, aby boli tieto prenosy zakázané. Tvrdil, že právo a prax Spojených štátov nezabezpečujú dostatočnú ochranu údajov prenesených do tejto krajiny pred prístupom zo strany orgánov verejnej moci tejto krajiny. Táto sťažnosť bola zamietnutá najmä z dôvodu, že Komisia vo svojom rozhodnutí 2000/520[79] konštatovala, že Spojené štáty zabezpečovali primeranú úroveň ochrany. Súdny dvor svojím rozsudkom zo 6. októbra 2015 v rámci rozhodovania o prejudiciálnej otázke, ktorú mu položil High Court (Vyšší súd, Írsko), rozhodol o neplatnosti tohto rozhodnutia (ďalej len „rozsudok Schrems I“).[80]

V nadväznosti na rozsudok Schrems I a následné zrušenie rozhodnutia o zamietnutí sťažnosť pána Schremsa írskym súdom, bol pán Schrems írskym dozorným orgánom vyzvaný, aby preformuloval svoju sťažnosť vzhľadom na zrušenie rozhodnutia 2000/520 Súdnym dvorom. Pán Schrems vo svojej preformulovanej sťažnosti tvrdí, že Spojené štáty nezabezpečujú dostatočnú ochranu údajov prenesených do tejto krajiny. Navrhuje pozastaviť alebo zakázať do budúcnosti prenos týchto údajov z Únie do Spojených štátov, ktorý Facebook Ireland v tom čase vykonával na základe štandardných doložiek o ochrane údajov uvedených v prílohe k rozhodnutiu 2010/87/EÚ[81]. Keďže írsky dozorný orgán dospel k záveru, že konanie o sťažnosti pána Schremsa závisí najmä od platnosti rozhodnutia 2010/87, začal konanie na High Court (Vyšší súd), aby tento súd predložil Súdnemu dvoru návrh na začatie prejudiciálneho konania. Po začatí tohto konania Komisia prijala rozhodnutie (EÚ) 2016/1250 o primeranosti ochrany poskytovanej štítom na ochranu osobných údajov medzi EÚ a USA[82].

Vnútroštátny súd sa svojím návrhom na začatie prejudiciálneho konania pýta Súdneho dvora na uplatniteľnosť GDPR na prenosy osobných údajov založené na štandardných doložkách o ochrane údajov uvedených v rozhodnutí 2010/87, na úroveň ochrany vyžadovanú týmto nariadením v rámci takého prenosu a na povinnosti zaväzujúce v tejto súvislosti dozorné orgány. High Court (Vyšší súd) sa okrem toho pýta na platnosť tak rozhodnutia 2010/87, ako aj rozhodnutia 2016/1250.

---

78 Článok 49 GDPR.

79 Rozhodnutie Komisie z 26. júla 2000 v súlade so smernicou Európskeho parlamentu a Rady 95/46/ES o primeranosti ochrany poskytovanej zásadami „bezpečného prístavu“ a súvisiacimi často kladenými otázkami vydanými Ministerstvom obchodu USA (Ú. v. EÚ L 215, 2000, s. 7; Mim. vyd. 16/001, s. 119).

80 Rozsudok Súdneho dvora zo 6. októbra 2015, Schrems, C-362/14, *EU:C:2015:650*.

81 Rozhodnutie Komisie z 5. februára 2010 o štandardných zmluvných doložkách pre prenos osobných údajov spracovateľom usadeným v tretích krajinách podľa smernice Európskeho parlamentu a Rady 95/46/ES (Ú. v. EÚ L 39, 2010, s. 5), zmenené vykonávacím rozhodnutím Komisie (EÚ) 2016/2297 zo 16. decembra 2016 (Ú. v. EÚ L 344, 2016, s. 100).

82 Vykonávacie rozhodnutie Komisie z 12. júla 2016 podľa smernice Európskeho parlamentu a Rady 95/46/ES o primeranosti ochrany poskytovanej štítom na ochranu osobných údajov medzi EÚ a USA (Ú. v. EÚ L 207, 2016, s. 1).

Súdny dvor konštatoval, že z preskúmania rozhodnutia 2010/87 z hľadiska Charty nevyplýva žiadna skutočnosť, ktorá by mohla ovplyvniť jeho platnosť. Naopak, rozhodnutie Komisie 2016/1250 vyhlásil za neplatné.

Súdny dvor v prvom rade konštatoval, že právo Únie a najmä GDPR sa uplatní na prenos osobných údajov vykonaný na obchodné účely hospodárskym subjektom usadeným v jednom členskom štáte inému hospodárskemu subjektu usadenému v tretej krajine, napriek tomu, že v priebehu tohto prenosu alebo po ňom môžu byť uvedené údaje spracúvané orgánmi dotknutej tretej krajiny na účely verejnej bezpečnosti, obrany a bezpečnosti štátu. Spresnil, že tento druh spracovania údajov orgánmi tretej krajiny nemôže vylúčiť taký prenos z pôsobnosti GDPR.

Pokiaľ ide o úroveň ochrany vyžadovanú v rámci takého prenosu, Súdny dvor rozhodol, že požiadavky stanovené na tento účel ustanoveniami GDPR, ktoré sa vzťahujú na primerané záruky, vymožiteľné práva a účinné právne prostriedky nápravy, sa majú vykladať v tom zmysle, že musia zabezpečiť, aby práva osôb, ktorých osobné údaje sa prenášajú do tretej krajiny na základe štandardných doložiek o ochrane údajov, požívali úroveň ochrany, ktorá je v podstate rovnocenná úrovni ochrany zaručenej v rámci Únie týmto nariadením v spojení s Chartou. V tejto súvislosti spresnil, že posúdenie tejto úrovne ochrany musí zohľadniť tak zmluvné ustanovenia dohodnuté medzi vývozcom údajov usadeným v Únii a príjemcom prenosu usadeným v dotknutej tretej krajine, ako aj, pokiaľ ide o prípadný prístup orgánov verejnej moci tejto tretej krajiny k takto prenášaným údajom, relevantné prvky právneho systému danej krajiny.

Pokiaľ ide o povinnosti zaväzujúce dozorné orgány v súvislosti s takýmto prenosom, Súdny dvor rozhodol, že pokiaľ neexistuje rozhodnutie o primeranosti, ktoré Komisia platne prijala, tieto orgány sú najmä povinné pozastaviť alebo zakázať prenos osobných údajov do tretej krajiny, ak sa vzhľadom na osobitné okolnosti tohto prenosu domnievajú, že štandardné doložky o ochrane údajov nie sú alebo nemôžu byť v tejto tretej krajine dodržané a že ochrana prenesených údajov vyžadovaná podľa práva Únie nemôže byť zabezpečená inými prostriedkami, pokiaľ vývozca so sídlom v Únii sám tento prenos nepozastaví alebo neukončí.

Súdny dvor ďalej preskúmal platnosť rozhodnutia 2010/87. Podľa Súdneho dvora len samotná skutočnosť, že štandardné doložky o ochrane údajov uvedené v tomto rozhodnutí nezaväzujú z dôvodu ich zmluvnej povahy orgány tretích krajín, do ktorých môžu byť osobné údaje prenesené, nemôže byť dôvodom na pochybnosti o platnosti tohto rozhodnutia. Táto platnosť naopak závisí od toho, či uvedené rozhodnutie obsahuje účinné mechanizmy, ktoré v praxi umožňujú zabezpečiť, aby bola dodržaná úroveň ochrany vyžadovaná právom Únie a aby sa prenosy osobných údajov založené na takýchto doložkách v prípade ich porušenia alebo nemožnosti ich dodržať pozastavili alebo zakázali. Súdny dvor konštatoval, že rozhodnutie 2010/87 takéto mechanizmy zavádza. V tejto súvislosti najmä zdôraznil, že toto rozhodnutie ukladá vývozcovi údajov a príjemcovi prenosu povinnosť vopred overiť, či sa v dotknutej tretej krajine táto úroveň ochrany dodržiava, a zaväzuje vývozcu údajov informovať tohto príjemcu o jeho

prípadnej nemožnosti zabezpečiť dodržanie štandardných doložiek o ochrane, pričom povinnosťou tohto vývozcu je vtedy pozastaviť prenos údajov a/alebo vypovedať zmluvu uzavretú s príjemcom.

Súdny dvor napokon preskúmal platnosť rozhodnutia 2016/1250 s ohľadom na požiadavky vyplývajúce z GDPR v spojení s ustanoveniami Charty, ktorými sa zaručuje rešpektovanie súkromného a rodinného života, ochrana osobných údajov a právo na účinnú súdnu ochranu. V tejto súvislosti Súdny dvor uviedol, že toto rozhodnutie podobne ako rozhodnutie 2000/520 stanovuje prednosť požiadaviek týkajúcich sa národnej bezpečnosti, verejného záujmu a dodržiavania právnych predpisov Spojených štátov, čím sa umožňuje zasahovanie do základných práv osôb, ktorých údaje sa do tejto tretej krajiny prenášajú. Podľa Súdneho dvora obmedzenia ochrany osobných údajov, ktoré vyplývajú z vnútroštátnej právnej úpravy Spojených štátov týkajúcej sa prístupu a používania takýchto údajov prenášaných z Únie do tejto tretej krajiny americkými orgánmi verejnej moci a ktoré Komisia posúdila v rozhodnutí 2016/1250, nie sú vymedzené takým spôsobom, aby zodpovedali požiadavkám, ktoré sú v podstate rovnocenné požiadavkám vyžadovaným v práve Únie zásadou proporcionality, pretože programy sledovania založené na tejto právnej úprave sa neobmedzujú na to, čo je striktne nevyhnutné. Na základe konštatovaní uvedených v danom rozhodnutí Súdny dvor uviedol, že v prípade niektorých programov sledovania z uvedenej právnej úpravy nijako nevyplýva, že by oprávnenie, ktoré obsahuje pre vykonávanie týchto programov, bolo akokoľvek obmedzené, a ani to, že by existovali záruky pre osoby, ktoré nie sú americkými občanmi a ktorých sa môžu tieto programy týkať. Súdny dvor dodal, že hoci tá istá právna úprava stanovuje požiadavky, ktoré musia americké orgány dodržiavať pri vykonávaní dotknutých programov sledovania, nepriznáva dotknutým osobám práva uplatniteľné pred súdmi voči týmto orgánom.

Pokiaľ ide o požiadavku súdnej ochrany, Súdny dvor rozhodol, že na rozdiel od toho, k čomu dospela Komisia v rozhodnutí 2016/1250, mechanizmus ombudsmana uvedený v tomto rozhodnutí neposkytuje opravný prostriedok pred orgánom, ktorý by ponúkal osobám, ktorých údaje sa prenášajú do Spojených štátov, záruky, ktoré sú v podstate rovnocenné zárukám vyžadovaným v práve Únie, v tom zmysle, že by zaručoval tak nezávislosť ombudsmana stanoveného týmto mechanizmom, ako aj existenciu noriem oprávňujúcich uvedeného ombudsmana prijímať záväzné rozhodnutia voči spravodajským službám Spojených štátov. Na základe všetkých týchto dôvodov Súdny dvor vyhlásil rozhodnutie 2016/1250 za neplatné.

V. Ochrana osobných údajov na internete

1. Právo na vznesenie námietky proti spracovaniu osobných údajov („právo na zabudnutie“)

Rozsudok z 13. mája 2014 (veľká komora), Google Spain a Google (C-131/12, EU:C:2014:317)

V tomto rozsudku (pozri tiež rubriky II.1. et II.3., nazvané „Pôsobnosť všeobecnej právnej úpravy“ a „Pojem ‚spracovanie osobných údajov‘“) Súdny dvor spresnil rozsah práva na prístup a práva na vznesenie námietky proti spracovaniu osobných údajov na internete, ktoré stanovuje smernica 95/46.

Súdny dvor v rámci toho, ako sa vyslovil k otázke rozsahu zodpovednosti poskytovateľa internetového vyhľadávača, v podstate rozhodol, že na účely dodržania práv na prístup a na vznesenie námietok, ktoré sú zaručené v článku 12 písm. b) a článku 14 prvom odseku písm. a) smernice 95/46, a pokiaľ sú podmienky stanovené v týchto článkoch skutočne splnené, je poskytovateľ vyhľadávača za určitých podmienok povinný odstrániť zo zoznamu výsledkov, ktoré sa zobrazia v nadväznosti na vyhľadávanie uskutočnené na základe zadania mena určitej osoby, odkazy na webové stránky uverejnené tretími osobami, ktoré obsahujú informácie týkajúce sa tejto osoby. Súdny dvor spresnil, že táto povinnosť môže existovať aj za predpokladu, že toto meno a tieto informácie nie sú ešte predtým alebo súčasne vymazané z týchto webových stránok, a to prípadne aj vtedy, ak je ich uverejnenie na uvedených stránkach ako také v súlade s právnymi predpismi.

Navyše Súdny dvor v odpovedi na otázku, či smernica umožňuje dotknutej osobe vyžadovať odstránenie odkazov na webové stránky zo zoznamu výsledkov z dôvodu, že si želá, aby tam uvedené informácie, ktoré sa jej týkajú, boli po určitom čase „zabudnuté“, najskôr uviedol, že aj spracovanie správnych údajov, ktoré bolo pôvodne v súlade s právnymi predpismi, sa môže časom stať nezlučiteľné s touto smernicou, pokiaľ tieto údaje už nie sú potrebné vzhľadom na účely, pre ktoré boli zhromaždené alebo spracované, a to najmä pokiaľ sa tieto údaje javia ako neadekvátne, nerelevantné alebo už nerelevantné, alebo neprimerané vo vzťahu k účelom ich spracovania a k uplynutému času. V dôsledku toho ak sa v nadväznosti na žiadosť dotknutej osoby konštatuje, že zahrnutie týchto odkazov na zoznam výsledkov je za súčasného stavu nezlučiteľné so smernicou, informácie a odkazy nachádzajúce sa na uvedenom zozname výsledkov musia byť vymazané. V tomto kontexte konštatovanie práva dotknutej osoby na to, aby informácia týkajúca sa jej osoby už nebola prepojená s jej menom prostredníctvom zoznamu výsledkov, nepredpokladá, aby zahrnutie dotknutej informácie na zoznam výsledkov spôsobovalo dotknutej osobe ujmu.

Napokon Súdny dvor spresnil, že keďže dotknutá osoba môže vzhľadom na svoje základné práva podľa článkov 7 a 8 Charty žiadať, aby dotknutá informácia už nebola sprístupnená širokej verejnosti prostredníctvom jej zahrnutia na takýto zoznam výsledkov, potom tieto práva v zásade prevažujú nielen nad hospodárskym záujmom

prevádzkovateľa vyhľadávača, ale aj nad záujmom verejnosti na nájdení uvedenej informácie v rámci vyhľadávania týkajúceho sa mena tejto osoby. To však neplatí v prípade, ak sa z osobitných dôvodov, akým je úloha uvedenej osoby vo verejnom živote, zistí, že zásah do jej základných práv je odôvodnený prevažujúcim záujmom uvedenej verejnosti na prístupe k predmetnej informácii prostredníctvom takéhoto zahrnutia.

2. Spracovanie osobných údajov a práva duševného vlastníctva

Rozsudok z 29. januára 2008 (veľká komora), Promusicae (C-275/06, EU:C:2008:54)

Promusicae, španielske neziskové združenie zastupujúce výrobcov a vydavateľov hudobných, ako aj audiovizuálnych nahrávok, sa obrátilo na španielske súdy, aby bola spoločnosti Telefónica de España SAU (obchodná spoločnosť, ktorej činnosť spočíva najmä v poskytovaní služieb prístupu k internetu) uložená povinnosť zverejniť totožnosť a adresu bydliska určitých osôb, ktorým táto spoločnosť poskytovala služby prístupu na internet a ktorých IP adresa, ako aj dátum a čas pripojenia boli známe. Podľa združenia Promusicae tieto osoby používali program na výmenu súborov, tzv. „peer-to-peer“ alebo „P2P“ (transparentný prostriedok zdieľania obsahu, ktorý je nezávislý, decentralizovaný a vybavený pokročilými funkciami vyhľadávania a sťahovania), a poskytovali v zdieľanom adresári svojho osobného počítača prístup k zvukovým záznamom, ku ktorým patria členom združenia Promusicae majetkové práva užívať tieto diela. Združenie preto požadovalo zverejnenie týchto informácií, aby mohlo proti dotknutým osobám začať občianskoprávne konania.

Práve za týchto podmienok Juzgado de lo Mercantil n° 5 de Madrid (Obchodný súd č. 5 Madrid, Španielsko) položil Súdnemu dvoru otázku, či európska právna úprava ukladá členským štátom, aby na účely zabezpečenia účinnej ochrany autorského práva stanovili povinnosť oznámiť osobné údaje v rámci občianskoprávneho konania.

Podľa Súdneho dvora v súvislosti s uvedeným návrhom na začatie prejudiciálneho konania vznikla otázka nevyhnutného vyváženia požiadaviek spojených s ochranou rôznych základných práv, a to jednak práva na rešpektovanie súkromného života a jednak práva na ochranu vlastníctva a práva na účinnú súdnu ochranu.

Súdny dvor v tejto súvislosti usúdil, že smernica 2000/31/ES o určitých právnych aspektoch služieb informačnej spoločnosti na vnútornom trhu, najmä o elektronickom obchode (smernica o elektronickom obchode)[83], smernica 2001/29/ES o zosúladení niektorých aspektov autorských práv a s nimi súvisiacich práv v informačnej

[83] Smernica Európskeho parlamentu a Rady 2000/31/ES z 8. júna 2000 o určitých právnych aspektoch služieb informačnej spoločnosti na vnútornom trhu, najmä o elektronickom obchode (smernica o elektronickom obchode) (Ú. v. ES L 178, 2000, s. 1; Mim. vyd. 13/025, s. 399).

spoločnosti[84], smernica 2004/48/ES o vymožiteľnosti práv duševného vlastníctva[85] a smernica 2002/58 neukladajú členským štátom, aby v takej situácii ako v konaní vo veci samej stanovili povinnosť oznámiť osobné údaje na účely zabezpečenia účinnej ochrany autorského práva v rámci občianskoprávneho konania. Právo Únie však od uvedených štátov pri preberaní týchto smerníc požaduje, aby vychádzali z ich výkladu, ktorý umožňuje zabezpečiť náležitú rovnováhu medzi rôznymi základnými právami chránenými právnym poriadkom Spoločenstva. Ďalej je potrebné, aby orgány a súdy členských štátov pri vykonávaní opatrení na prebratie uvedených smerníc nielen vykladali svoje vnútroštátne právo v súlade s týmito smernicami, ale takisto, aby nevychádzali z výkladu týchto smerníc, ktorý by kolidoval s uvedenými základnými právami alebo s inými všeobecnými zásadami práva Spoločenstva, ako je zásada proporcionality.

Rozsudok z 19. apríla 2012, Bonnier Audio a i. (C-461/10, EU:C:2012:219)

Högsta domstolen (Najvyšší súd, Švédsko) sa obrátil na Súdny dvor s návrhom na začatie prejudiciálneho konania v súvislosti s výkladom smerníc 2002/58 a 2004/48 v rámci sporu medzi spoločnosťami Bonnier Audio AB, Earbooks AB, Norstedts Förlagsgrupp AB, Piratförlaget AB a Storyside AB (ďalej len „Bonnier Audio a i.“) a spoločnosťou Perfect Communication Sweden AB (ďalej len „ePhone“) vo veci, v ktorej ePhone namietala proti návrhu na vydanie príkazu oznámiť údaje, ktorý podali Bonnier Audio a i.

V tejto veci sú Bonnier Audio a i. vydavatelia, ktorí majú výlučné práva vyhotovovať rozmnoženiny, spracovávať a sprístupňovať verejnosti 27 diel vo forme audiokníh. Bonnier Audio a i. tvrdili, že ich výlučné práva boli porušené osobou, ktorá týchto 27 diel sprístupňovala verejnosti bez ich súhlasu prostredníctvom servera FTP („file transfer protocol“), ktorý umožňuje sprístupňovanie súborov a prenos údajov medzi počítačmi pripojenými k internetu. Bonnier Audio a i. preto podali na švédske súdy návrh na vydanie príkazu na oznámenie mena a adresy osoby využívajúcej adresu IP, z ktorej boli údajne zaslané dotknuté súbory.

V tomto kontexte sa Högsta domstolen (Najvyšši súd) rozhodujúci o kasačnom opravnom prostriedku obrátil na Súdny dvor s otázkou, či právo Únie bráni uplatneniu vnútroštátneho ustanovenia, ktoré sa zakladá na článku 8 smernice 2004/48, ktorá povoľuje, aby bolo poskytovateľovi internetových služieb v rámci občianskoprávneho konania na účely identifikácie konkrétneho účastníka internetu prikázané oznámiť majiteľovi alebo držiteľovi autorských práv informácie o identite účastníka, ktorému poskytovateľ internetového pripojenia pridelil určitú adresu IP, ktorá bola údajne použitá pri porušení uvedeného práva. Predpokladalo sa, že jednak navrhovateľ vydania príkazu

[84] Smernica Európskeho parlamentu a Rady 2001/29/ES z 22. mája 2001 o zosúladení niektorých aspektov autorských práv a s nimi súvisiacich práv v informačnej spoločnosti (Ú. v. ES L 167, 2001, s. 10; Mim. vyd. 17/001, s. 230).

[85] Smernica Európskeho parlamentu a Rady 2004/48/ES z 29. apríla 2004 o vymožiteľnosti práv duševného vlastníctva (Ú. v. EÚ L 157, 2004, s. 45; Mim. vyd. 17/002, s. 32).

predložil dôkazy o porušení autorského práva a jednak že požadované opatrenie bolo primerané.

Súdny dvor najskôr pripomenul, že článok 8 ods. 3 smernice 2004/48 v spojení s článkom 15 ods. 1 smernice 2002/58 síce nebráni tomu, aby členské štáty stanovili povinnosť poskytovať osobné údaje súkromným osobám na účely postihu porušenia autorského práva pred občianskoprávnymi súdmi, avšak týmto štátom neukladá povinnosť, aby takú povinnosť stanovili. Orgánom a súdom členských štátov však prináleží, aby nielen vykladali svoje vnútroštátne právo v súlade s týmito smernicami, ale takisto dbali na to, aby nevychádzali z výkladu týchto smerníc, ktorý by kolidoval s uvedenými základnými právami alebo s inými všeobecnými zásadami práva Únie, ako je zásada proporcionality.

Súdny dvor v tejto súvislosti konštatoval, že podľa dotknutej vnútroštátnej právnej úpravy sa na účely vydania príkazu oznámiť predmetné údaje predovšetkým vyžadovalo, aby existovali nesporné dôkazy o porušení práv duševného vlastníctva, aby tieto informácie mohli uľahčiť vyšetrovanie porušenia práva duševného vlastníctva alebo jeho narušenia a aby dôvody takého príkazu prevažovali nad prípadnými nevýhodami alebo inou ujmou, ktoré toto opatrenie môže spôsobiť jeho adresátovi alebo akémukoľvek protichodnému záujmu.

V dôsledku toho Súdny dvor dospel k záveru, že smernice 2002/58 a 2004/48 nebránia takej vnútroštátnej právnej úprave, akou je právna úprava vo veci samej, pokiaľ vnútroštátnemu súdu, ktorému aktívne legitimovaný subjekt predložil návrh na vydanie príkazu poskytnúť osobné údaje, umožňuje, aby v závislosti od okolností každého samostatného prípadu a s náležitým prihliadnutím na požiadavky vyplývajúce zo zásady proporcionality zvážil jednotlivé protichodné záujmy.

3. Odstránenie odkazov na osobné údaje

Rozsudok z 24. septembra 2019 (veľká komora), GC a i. (Odstránenie odkazov na citlivé údaje) (C-136/17, ***EU:C:2019:773)***

V tomto rozsudku Súdny dvor zasadajúci vo veľkej komore spresnil povinnosti poskytovateľa vyhľadávača v rámci žiadosti o odstránenie odkazov týkajúcich sa citlivých údajov.

Spoločnosť Google odmietla vyhovieť žiadostiam štyroch osôb, aby z výsledkov vyhľadávania, ktoré sa zobrazujú pri zadaní ich mena do vyhľadávača, odstránila rôzne odkazy vedúce na webové stránky zverejnené tretími osobami, najmä na články uverejnené v tlači. V nadväznosti na sťažnosti, ktoré tieto štyri osoby podali, Commission nationale de l'informatique a des libertés (Národná komisia pre informačné technológie a slobody, CNIL, Francúzsko) odmietla uložiť spoločnosti Google povinnosť odstrániť

príslušné odkazy. Conseil d'État (Štátna rada, Francúzsko), ktorá rozhodovala o tejto veci, požiadala Súdny dvor o spresnenie povinností poskytovateľa internetového vyhľadávača pri vybavovaní žiadosti o odstránenie odkazu podľa smernice 95/46.

Súdny dvor v prvom rade pripomenul, že spracúvanie osobných údajov prezrádzajúcich rasový alebo etnický pôvod, politické názory, náboženské alebo filozofické presvedčenia, členstvo v odborových zväzoch, ako aj spracúvanie údajov týkajúcich sa zdravia alebo sexuálneho života, je zakázané,[86] s výhradou určitých výnimiek a odchýlok. Spracúvanie údajov týkajúcich sa trestných činov, odsúdení v trestnom konaní alebo bezpečnostných opatrení možno vykonávať iba pod kontrolou orgánu verejnej moci, alebo ak vnútroštátne právo ustanovuje vhodné osobitné záruky.[87]

Súdny dvor rozhodol, že zákaz a obmedzenia týkajúce sa spracúvania osobitných kategórií údajov sa uplatňujú na poskytovateľa internetového vyhľadávača rovnako ako na každého iného prevádzkovateľa zodpovedného za spracúvanie osobných údajov. Účelom týchto zákazov a obmedzení je totiž zabezpečiť zvýšenú ochranu v prípade takéhoto spracúvania, ktoré môže vzhľadom na osobitnú citlivosť týchto údajov predstavovať obzvlášť závažný zásah do základných práv na ochranu súkromia a na ochranu osobných údajov.

Poskytovateľ vyhľadávača však nenesie zodpovednosť z dôvodu, že na webovej stránke zverejnenej treťou osobou sa nachádzajú osobné údaje, ale z dôvodu, že na takúto stránku odkazuje. Za týchto podmienok sa zákaz a obmedzenia týkajúce sa spracúvania citlivých údajov uplatnia na tohto poskytovateľa len z titulu takéhoto odkazovania, a to v rámci overovania, ktoré sa má uskutočniť pod dohľadom príslušných vnútroštátnych orgánov na základe žiadosti dotknutej osoby.

V druhom rade Súdny dvor dospel k záveru, že ak je poskytovateľovi vyhľadávača podaná žiadosť o odstránenie odkazov týkajúca sa citlivých údajov, s výhradou určitých výnimiek je v zásade povinný jej vyhovieť. Pokiaľ ide o tieto výnimky, poskytovateľ môže odmietnuť vyhovieť takejto žiadosti najmä vtedy, ak konštatuje, že odkazy vedú na údaje, ktoré zjavne zverejnila dotknutá osoba,[88] a to pod podmienkou, že uvádzanie týchto odkazov spĺňa ostatné podmienky prípustnosti spracúvania osobných údajov a s výnimkou prípadu, keď má táto osoba právo namietať proti uvedenému uvádzaniu odkazov z dôvodov týkajúcich sa jej osobitnej situácie.[89]

V každom prípade, ak je poskytovateľovi vyhľadávača predložená žiadosť o odstránenie odkazu, je povinný overiť, či sa zahrnutie odkazu na webovú stránku, na ktorej sú uverejnené citlivé osobné údaje, do zoznamu výsledkov zobrazovaného po zadaní mena tejto osoby do vyhľadávača javí ako striktne nevyhnutné pre ochranu práva na informácie v prípade tých používateľov internetu, ktorí by potenciálne mohli mať záujem

[86] Článok 8 ods. 1 smernice 95/46 a článok 9 ods. 1 nariadenia 2016/679.
[87] Článok 8 ods. 5 smernice 95/46 a článok 10 nariadenia 2016/679.
[88] Článok 8 ods. 2 písm. e) smernice 95/46 a článok 9 ods. 2 písm. e) nariadenia 2016/679.
[89] Článok 14 prvý odsek písm. a) smernice 95/46 a článok 21 ods. 1 nariadenia 2016/679.

o prístup na túto webovú stránku prostredníctvom takéhoto vyhľadávania. Súdny dvor v tejto súvislosti zdôraznil, že hoci práva na rešpektovanie súkromia a ochranu osobných údajov vo všeobecnosti prevažujú nad právom používateľov internetu na informácie, táto rovnováha môže v konkrétnych prípadoch závisieť od povahy predmetnej informácie a od jej citlivosti pre súkromný život dotknutej osoby, ako aj od záujmu verejnosti disponovať touto informáciou, ktorý sa môže líšiť najmä v závislosti od úlohy tejto osoby vo verejnom živote.

V treťom rade Súdny dvor rozhodol, že je úlohou poskytovateľa vyhľadávača, aby v rámci žiadosti o odstránenie odkazov na údaje týkajúce sa súdneho konania v trestnej veci vedeného voči dotknutej osobe, ktoré sa vzťahujú na predchádzajúcu etapu predmetného konania a už nezodpovedajú aktuálnej situácii, posúdil, či vzhľadom na všetky okolnosti danej veci má uvedená osoba právo na to, aby dotknuté informácie už neboli v súčasnom štádiu spájané s jej menom prostredníctvom zoznamu výsledkov zobrazovaného po zadaní jej mena do vyhľadávača. Hoci o takýto prípad nejde z dôvodu, že zahrnutie predmetného odkazu je striktne nevyhnutné na zosúladenie práv na ochranu súkromia a na ochranu osobných údajov dotknutej osoby s právom na informácie potenciálne dotknutých používateľov internetu, prevádzkovateľ je aj napriek tomu povinný najneskôr v prípade, že sa vyskytne žiadosť o odstránenie odkazu, usporiadať zoznam výsledkov tak, aby celkový obraz, ktorý z neho bude vyplývať pre používateľa internetu, odrážal aktuálnu právnu situáciu, čo si osobitne vyžaduje, aby boli odkazy na internetové stránky obsahujúce informácie v tejto súvislosti uvedené v tomto zozname na prvom mieste.

***Rozsudok z 24. septembra 2019 (veľká komora), Google (Územná pôsobnosť odstránenia odkazov) (C-507/17,* EU:C:2019:772)**

Commission nationale de l'informatique et des libertés (Národná komisia pre informačné technológie a občianske slobody, CNIL, Francúzsko) vyzvala Google, aby v rámci vyhovenia žiadosti o odstránenie odkazov vedúcich na webové stránky obsahujúce osobné údaje dotknutej osoby zo zoznamu výsledkov zobrazených v nadväznosti na vyhľadávanie uskutočnené na základe zadania jej mena, odstránila tieto odkazy na všetkých koncovkách doménového mena svojho vyhľadávača. Po tom, čo Google odmietla vyhovieť uvedenej výzve, jej CNIL uložila sankciu vo výške 100 000 eur. Conseil d'État (Štátna rada, Francúzsko), na ktorú sa obrátila Google, požiadala Súdny dvor o spresnenie územnej pôsobnosti povinnosti prevádzkovateľa vyhľadávača pri vykonaní práva na odstránenie odkazov podľa smernice 95/46.

Súdny dvor najprv pripomenul možnosť fyzických osôb uplatniť na základe práva Únie svoje právo na odstránenie odkazov voči poskytovateľovi vyhľadávača, ktorý má jednu alebo viaceré prevádzkarne na území Únie nezávisle od toho, či k tomuto spracúvaniu osobných údajov (v tomto prípade odkazov na webové stránky, na ktorých sú uvedené

osobné údaje týkajúce sa osoby, ktorá sa tohto práva dovoláva), dochádza alebo nedochádza v Únii.[90]

Pokiaľ ide o rozsah práva na odstránenie odkazov, Súdny dvor konštatoval, že poskytovateľ vyhľadávača nie je povinný urobiť toto odstránenie vo všetkých verziách svojho vyhľadávača, ale len v jeho verziách zodpovedajúcich všetkým členským štátom. V tejto súvislosti uviedol, že hoci by úplné odstránenie odkazov v celom rozsahu spĺňalo so zreteľom na charakteristiky internetu a vyhľadávačov cieľ normotvorcu Únie spočívajúci v zabezpečení vysokej úrovne ochrany osobných údajov v celej Únii, z práva Únie nijako nevyplýva,[91] že by normotvorca Únie na účely zabezpečenia dosiahnutia takého cieľa rozhodol, že právu na odstránenie odkazov prizná pôsobnosť, ktorá by prekračovala územie členských štátov. Konkrétne, zatiaľ čo právo Únie zavádza mechanizmy spolupráce medzi dozornými orgánmi členských štátov na účely dosiahnutia spoločného rozhodnutia založeného na vyvážení jednak práva na ochranu súkromného života a ochranu osobných údajov a jednak záujmu verejnosti pochádzajúcej z rôznych členských štátov na prístupe k informáciám, takéto mechanizmy nie sú v súčasnosti stanovené, pokiaľ ide o rozsah práva na odstránenia odkazov mimo Únie.

V súčasnosti je podľa práva Únie úlohou poskytovateľa vyhľadávača, aby pristúpil k požadovanému odstráneniu odkazov, a to nielen v jednej verzii vyhľadávača zodpovedajúcej členskému štátu, v ktorom má osoba s nárokom na odstránenie odkazov bydlisko, ale vo verziách vyhľadávača zodpovedajúcich členským štátom, a to s cieľom zabezpečiť konzistentnú a vysokú úroveň ochrany v celej Únii. Okrem toho takémuto poskytovateľovi navyše prináleží, aby v prípade potreby prijal dostatočne účinné opatrenia na zabránenie alebo prinajmenšom vážne odradenie používateľov internetu pochádzajúcich z Únie od prístupu – aj prostredníctvom verzie vyhľadávača zodpovedajúcej tretím štátom – k odkazom, ktoré sú predmetom odstránenia odkazov, a vnútroštátnemu súdu prináleží overiť, či opatrenia prijaté poskytovateľom túto požiadavku spĺňajú.

Napokon Súdny dvor zdôraznil, že právo Únie síce neukladá poskytovateľovi vyhľadávača vykonať odstránenie vo všetkých verziách jeho vyhľadávača, no ani to nezakazuje. Dozorný orgán alebo súdny orgán členského štátu má teda naďalej právomoc vykonať s ohľadom na vnútroštátne štandardy ochrany základných práv vyváženie medzi jednak právom dotknutej osoby na rešpektovanie jej súkromného života a na ochranu osobných údajov, ktoré sa jej týkajú, a jednak právom na informácie, ako aj na základe tohto vyváženia prípadne uložiť poskytovateľovi vyhľadávača povinnosť odstrániť odkazy, ktorá sa vzťahuje na všetky verzie uvedeného vyhľadávača.

[90] Článok 4 ods. 1 písm. a) smernice 95/46 a článok 3 ods. 1 nariadenia 2016/679.
[91] Článok 12 písm. b) a článok 14 prvý odsek písm. a) smernice 95/46 a článok 17 ods. 1 nariadenia 2016/679.

Rozsudok z 8. decembra 2022 (veľká komora), Google (Odstránenie údajne nesprávneho obsahu) (C-460/20, EU:C:2022:962)

Žalobcovia vo veci samej, TU, ktorý zastáva vedúce pozície a vlastní obchodné podiely v rôznych spoločnostiach, a RE, ktorá bola jeho družkou a až do mája 2015 prokuristkou jednej z týchto spoločností, boli predmetom troch článkov uverejnených v roku 2015 na internetovej stránke spoločnosťou G LLC, prevádzkovateľom tejto internetovej stránky. Tieto články, z ktorých jeden bol ilustrovaný štyrmi fotografiami, na ktorých figurujú žalobcovia a ktoré vyvolávajú dojem, že žalobcovia vedú luxusný život, kriticky prezentovali investičný model viacerých ich spoločností. Prístup k týmto článkom bol možný na základe zadania krstných mien a priezvisk žalobcov do vyhľadávača prevádzkovaného spoločnosťou Google LLC (ďalej len „Google“), a to tak samostatne, ako aj v spojení s niektorými názvami spoločností. Zoznam výsledkov odkazoval na tieto články prostredníctvom odkazu, ako aj na fotografie zobrazené vo forme miniatúr („thumbnails“).

Žalobcovia vo veci samej požiadali Google ako prevádzkovateľa osobných údajov, ktorých spracovanie sa uskutočňuje prostredníctvom jeho vyhľadávača, jednak o odstránenie odkazov na predmetné články zo zoznamu výsledkov vyhľadávania z dôvodu, že obsahujú nesprávne tvrdenia a hanlivé názory, a jednak o odstránenie miniatúr zo zoznamu výsledkov vyhľadávania. Google odmietla tejto žiadosti vyhovieť.

Žalobcovia vo veci samej, ktorých návrhy boli zamietnuté tak v konaní na prvom stupni, ako aj v odvolacom konaní, podali na Bundesgerichtshof (Spolkový súdny dvor, Nemecko) opravný prostriedok „Revision“, v rámci ktorého sa Bundesgerichtshof obrátil na Súdny dvor s návrhom na začatie prejudiciálneho konania, pokiaľ ide o výklad GDPR a smernice 95/46.[92]

Súdny dvor svojím rozsudkom, ktorý bol vydaný vo veľkej komore, rozvinul svoju judikatúru týkajúcu sa podmienok, ktoré sa uplatňujú na žiadosti o odstránenie odkazu adresované poskytovateľovi vyhľadávača, na základe pravidiel vzťahujúcich sa na ochranu osobných údajov. Konkrétne preskúmal jednak rozsah povinností a zodpovednosti, ktoré prináležia poskytovateľovi vyhľadávača pri vybavovaní žiadosti o odstránenie obsahu, ktorá je založená na údajnej nesprávnosti informácií uvedených v obsahu, na ktorý je zriadený odkaz, a jednak dôkazné bremeno, ktoré musí znášať dotknutá osoba, pokiaľ ide o túto nesprávnosť. Okrem toho sa vyjadril k potrebe toho, aby sa na účely preskúmania žiadosti o odstránenie fotografií zobrazených vo forme miniatúr v zozname výsledkov vyhľadávania obrázkov zohľadnil pôvodný kontext uverejnenia týchto fotografií na internete.

Súdny dvor v prvom rade rozhodol, že v rámci vyváženia, ktoré treba vykonať medzi právami na ochranu súkromia a ochranu osobných údajov na jednej strane a právom na

[92] Článok 17 ods. 3 písm. a) GDPR a článok 12 písm. b) a článok 14 prvý odsek písm. a) smernice 95/46.

slobodu prejavu a na informácie[93] na druhej strane, na účely preskúmania žiadosti o odstránenie odkazu, ktorá je adresovaná poskytovateľovi vyhľadávača a v ktorej sa žiada, aby sa zo zoznamu výsledkov vyhľadávania odstránil odkaz vedúci k obsahu zahŕňajúcemu údajne nesprávne informácie, toto odstránenie odkazu nepodlieha podmienke, aby otázka správnosti obsahu, na ktorý je zriadený odkaz, bola vyriešená aspoň predbežne v rámci žaloby podanej žiadateľom proti poskytovateľovi obsahu.

Hneď na úvod Súdny dvor na účely preskúmania, za akých podmienok je poskytovateľ vyhľadávača povinný vyhovieť žiadosti o to, aby sa odstránil, a teda vymazal zo zoznamu výsledkov zobrazovaného v nadväznosti na vyhľadávanie uskutočnené na základe zadania mena dotknutej osoby, odkaz na internetovú stránku, na ktorej sú uvedené tvrdenia, ktoré táto osoba považuje za nesprávne, okrem iného pripomenul toto:

• keďže činnosť vyhľadávača môže popri činnosti editorov internetových stránok významne ovplyvniť základné práva na ochranu súkromia a ochranu osobných údajov, poskytovateľ tohto vyhľadávača ako osoba, ktorá určuje ciele a prostriedky tejto činnosti, musí v rámci svojich zodpovedností, kompetencií a možností zaručiť, aby záruky stanovené smernicou 95/46 a GDPR mohli mať plný účinok a aby účinná a úplná ochrana dotknutých osôb mohla byť skutočne dosiahnutá,

• keď je poskytovateľovi vyhľadávača predložená žiadosť o odstránenie odkazu, tento poskytovateľ musí overiť, či je zahrnutie odkazu na predmetnú internetovú stránku do zoznamu výsledkov potrebné pre výkon práva na informácie, chráneného v rámci práva na slobodu prejavu a na informácie, v prípade tých používateľov internetu, ktorí by potenciálne mohli mať záujem o prístup na túto internetovú stránku prostredníctvom takéhoto vyhľadávania,

• GDPR výslovne zakotvuje požiadavku vyváženia medzi základnými právami na ochranu súkromia a ochranu osobných údajov na jednej strane a základným právom na informácie na druhej strane.

Súdny dvor predovšetkým poukazuje na to, že hoci práva dotknutej osoby na ochranu súkromia a ochranu osobných údajov vo všeobecnosti prevažujú nad legitímnym záujmom používateľov internetu na tom, aby mali k predmetnej informácii prístup, táto rovnováha môže závisieť od relevantných okolností každého jednotlivého prípadu, predovšetkým od povahy tejto informácie a od jej citlivosti pre súkromie dotknutej osoby, ako aj od záujmu verejnosti disponovať uvedenou informáciou, ktorý sa môže líšiť najmä v závislosti od úlohy, ktorú táto osoba zohráva vo verejnom živote.

Otázka správnosti alebo nesprávnosti obsahu, na ktorý je zriadený odkaz, je tiež relevantnou skutočnosťou v rámci tohto posúdenia. Za určitých okolností tak právo na informácie používateľov internetu a právo na slobodu prejavu poskytovateľa obsahu môžu prevážiť nad právami na ochranu súkromia a na ochranu osobných údajov, najmä

[93] Základné práva zaručené článkami 7, 8 a 11 Charty.

ak dotknutá osoba zohráva úlohu vo verejnom živote. Tento vzťah sa však obracia v prípade, že sa aspoň časť informácií, ktoré sú uvedené v žiadosti o odstránenie odkazu a ktorých dôležitosť nie je s ohľadom na celý obsah zanedbateľná, ukáže byť nesprávna. V takomto prípade by totiž právo šíriť informácie a právo dostávať informácie nebolo možné zohľadňovať, pretože tieto nemôžu zahŕňať aj právo na šírenie takýchto informácií a na prístup k nim.

Ďalej, pokiaľ ide po prvé o povinnosti týkajúce sa zistenia správnosti alebo nesprávnosti informácií uvedených v obsahu, na ktorý je zriadený odkaz, Súdny dvor spresnil, že osoba, ktorá žiada o odstránenie odkazu z dôvodu nesprávnosti takýchto informácií, je povinná preukázať zjavnú nesprávnosť týchto informácií, alebo prinajmenšom časti týchto informácií, ktorých dôležitosť nie je s ohľadom na celý obsah zanedbateľná. S cieľom zabrániť tomu, aby táto osoba znášala nadmerné bremeno, ktoré by mohlo narušiť potrebný účinok práva na odstránenie odkazu, však tejto osobe prináleží poskytnúť iba také dôkazy, pri ktorých je od nej vzhľadom na okolnosti prejednávanej veci možné primerane požadovať, aby ich zisťovala. Tejto osobe v zásade nemôže byť už v štádiu pred podaním žaloby uložená povinnosť, aby na podporu svojej žiadosti o odstránenie odkazu predložila súdne rozhodnutie vydané proti editorovi internetovej stránky, a to ani v podobe rozhodnutia vydaného v konaní o nariadení predbežného opatrenia.

Po druhé, pokiaľ ide o povinnosti a zodpovednosť poskytovateľa vyhľadávača, Súdny dvor zdôraznil, že tento sa na účely overenia toho, či v nadväznosti na žiadosť o odstránenie odkazu môže byť obsah naďalej zahrnutý v zozname výsledkov vyhľadávania uskutočneného prostredníctvom jeho vyhľadávača, musí opierať o všetky práva a záujmy, o ktoré ide, ako aj o všetky okolnosti prejednávanej veci. Tento poskytovateľ však nemôže byť povinný vyšetrovať skutkové okolnosti a na tento účel zorganizovať kontradiktórnu výmenu názorov s poskytovateľom obsahu s cieľom získať chýbajúce informácie o správnosti obsahu, na ktorý je zriadený odkaz. Povinnosť prispieť k preukázaniu správnosti alebo nesprávnosti obsahu, na ktorý je zriadený odkaz, by tohto poskytovateľa zaťažovala bremenom presahujúcim to, čo od neho možno rozumne očakávať vzhľadom na jeho zodpovednosť, právomoci a možnosti. Toto riešenie by tak so sebou prinášalo vážne riziko toho, že na obsahy, ktoré zodpovedajú legitímnej a prevažujúcej potrebe poskytovať informácie verejnosti, budú zrušené odkazy, a že sa tak sťaží ich vyhľadávanie na internete. Existovalo by tak skutočné riziko odradzujúceho účinku na výkon slobody prejavu a práva na informácie, ak by takýto poskytovateľ kvázi systematicky odstraňoval takéto odkazy s cieľom vyhnúť sa tomu, že by musel znášať bremeno vyšetrovania relevantných skutkových okolností na účely stanovenia správnosti alebo nesprávnosti obsahu, na ktorý je zriadený odkaz.

Preto v prípade, že žiadateľ o odstránenie odkazu predloží dôkazy preukazujúce zjavnú nesprávnosť informácií uvedených v obsahu, na ktorý je zriadený odkaz, alebo prinajmenšom časti týchto informácií, ktorých dôležitosť nie je s ohľadom na celý tento obsah zanedbateľná, poskytovateľ vyhľadávača je povinný tejto žiadosti vyhovieť. To isté

platí v prípade, že tento žiadateľ predloží súdne rozhodnutie prijaté proti editorovi internetovej stránky, ktoré je založené na konštatovaní, že informácie nachádzajúce sa v obsahu, na ktorý je zriadený odkaz a ktorých dôležitosť nie je s ohľadom na celý tento obsah zanedbateľná, sú prinajmenšom na prvý pohľad nesprávne. Naopak v prípade, že sa nesprávnosť takýchto informácií nezdá byť zjavná so zreteľom na dôkazy poskytnuté žiadateľom, takejto žiadosti o odstránenie odkazu nie je poskytovateľ vyhľadávača pri neexistencii takéhoto súdneho rozhodnutia povinný vyhovieť. Pokiaľ predmetné informácie môžu prispieť k diskusii vo verejnom záujme, je potrebné so zreteľom na všetky okolnosti konkrétneho prípadu priznať právu na slobodu prejavu a na informácie osobitný význam.

Napokon Súdny dvor dodal, že pokiaľ poskytovateľ vyhľadávača žiadosti o odstránenie odkazu nevyhovie, dotknutá osoba musí mať možnosť sa obrátiť na dozorný orgán alebo súdny orgán, aby tento uskutočnil nevyhnutné overenia a nariadil tomuto prevádzkovateľovi prijať potrebné opatrenia. V tejto súvislosti práve predovšetkým súdne orgány musia zabezpečiť zvažovanie protichodných záujmov, pretože tieto sú najpovolanejšie na vykonanie komplexného a dôkladného vyváženia, ktoré zohľadňuje všetky kritériá a všetky skutočnosti stanovené príslušnou judikatúrou.

Súdny dvor v druhom rade rozhodol, že v rámci vyváženia medzi vyššie uvedenými základnými právami je na účely preskúmania žiadosti o odstránenie odkazu, ktorou sa žiada, aby sa z výsledkov vyhľadávania obrázkov, uskutočneného na základe zadania mena fyzickej osoby, odstránili fotografie zobrazené vo forme miniatúr, na ktorých táto osoba figuruje, potrebné zohľadniť informatívnu hodnotu týchto fotografií bez ohľadu na pôvodný kontext ich uverejnenia na internetovej stránke, z ktorej sú vyňaté. Treba však prihliadnuť na všetky textové prvky, ktoré sú priamo pripojené k zobrazeniu týchto fotografií vo výsledkoch vyhľadávania a ktoré sú spôsobilé objasniť informačnú hodnotu týchto fotografií.

Pri tom, ako Súdny dvor dospel k tomuto záveru, zdôraznil, že vyhľadávanie obrázkov uskutočnené prostredníctvom internetového vyhľadávača na základe zadania mena osoby podlieha rovnakým zásadám, ako sú zásady uplatniteľné na vyhľadávanie internetových stránok a informácií, ktoré sú na nich obsiahnuté. Súdny dvor uviedol, že zobrazovanie fotografií dotknutej osoby vo forme miniatúr v nadväznosti na vyhľadávanie prostredníctvom zadania mena je takej povahy, že môže predstavovať mimoriadne významný zásah do práv na ochranu súkromia a osobných údajov tejto osoby.

Preto v prípade, že je poskytovateľovi vyhľadávača predložená žiadosť o odstránenie odkazu, ktorou sa žiada, aby sa z výsledkov vyhľadávania obrázkov vykonaného na základe zadania mena osoby odstránili fotografie zobrazené vo forme miniatúr, na ktorých táto osoba figuruje, daný poskytovateľ musí overiť, či je zobrazenie predmetných fotografií nevyhnutné na výkon práva na informácie používateľov internetu, ktorí majú potenciálne záujem o prístup k týmto fotografiám prostredníctvom takéhoto vyhľadávania.

Keďže pritom vyhľadávač zobrazuje fotografie dotknutej osoby mimo kontextu, v ktorom sú uverejnené na internetovej stránke, na ktorú je zriadený odkaz, a to najčastejšie na účely ilustrácie textových prvkov, ktoré táto stránka obsahuje, treba stanoviť, či sa tento kontext napriek tomu musí zohľadniť pri vyvažovaní protichodných práv a záujmov, ktoré sa má vykonať. V tomto rámci otázka, či má uvedené posúdenie zahŕňať aj obsah internetovej stránky, na ktorej sa nachádza fotografia, o ktorej odstránenie zobrazovania vo forme miniatúry sa žiada, závisí od predmetu a povahy predmetného spracúvania.

Pokiaľ ide po prvé o predmet daného spracúvania, Súdny dvor poznamenal, že uverejnenie fotografií ako neverbálneho prostriedku komunikácie môže mať na používateľov internetu výraznejší efekt ako uverejnenia textov. Fotografie sú totiž ako také dôležitým prostriedkom na pritiahnutie pozornosti používateľov internetu a môžu vzbudiť záujem o prístup k článkom, ktoré ilustrujú. Predovšetkým z dôvodu tej skutočnosti, že fotografie je často možné interpretovať viacerými spôsobmi, pritom ich zobrazenie v zozname výsledkov vyhľadávania ako miniatúr môže spôsobiť obzvlášť závažný zásah do práva dotknutej osoby na ochranu jej podobizne, čo treba v rámci vyvažovania protichodných práv a záujmov vziať do úvahy. Je potrebné uskutočniť osobitné vyváženie podľa toho, či ide na jednej strane o články opatrené fotografiami, ktoré uverejnil editor internetovej stránky a ktoré v prípade, že sú vložené do ich pôvodného kontextu, ilustrujú informácie poskytnuté v týchto článkoch a názory, ktoré sú v nich vyjadrené, a na druhej strane o fotografie zobrazené vo forme miniatúr v zozname výsledkov zo strany poskytovateľa vyhľadávača mimo rámca kontextu, v ktorom boli tieto fotografie uverejnené na pôvodnej internetovej stránke.

V tejto súvislosti Súdny dvor pripomenul, že nielenže sa dôvod odôvodňujúci uverejnenie osobných údajov na internetovej stránke nevyhnutne nemusí prekrývať s dôvodom, ktorý sa vzťahuje na činnosť vyhľadávača, ale že aj v takom prípade sa výsledok vyváženia dotknutých práv a záujmov, ktoré sa má vykonať, môže líšiť v závislosti od toho, či ide o spracovanie uskutočnené poskytovateľom vyhľadávača alebo spracovanie uskutočnené editorom tejto internetovej stránky. Na jednej strane legitímne záujmy odôvodňujúce tieto spracovania môžu byť odlišné a na druhej strane dôsledky, ktoré majú uvedené spracovania na dotknutú osobu a najmä na jeho súkromný život, nevyhnutne nie sú rovnaké.

Pokiaľ ide po druhé o povahu spracovania uskutočneného poskytovateľom vyhľadávača, Súdny dvor konštatoval, že tým, že poskytovateľ vyhľadávača vyhľadá fotografie fyzických osôb uverejnené na internete a zobrazí ich oddelene vo výsledkoch vyhľadávania obrázkov vo forme miniatúr, ponúka službu, ktorá zahŕňa spracovanie osobných údajov, ktoré je autonómne a samostatné vo vzťahu ku spracovaniu zo strany editora internetovej stránky, z ktorej sú fotografie vyňaté, ako aj ku spracovaniu, za ktoré tento poskytovateľ rovnako zodpovedá, týkajúcemu sa uvedenia odkazu na túto stránku.

V dôsledku uvedeného je nevyhnutné vykonať autonómne posúdenie činnosti poskytovateľa vyhľadávača spočívajúcej v zobrazení výsledkov vyhľadávania obrázkov vo forme miniatúr, pretože dodatočné porušenie základných práv, ktoré vyplýva z takejto

činnosti, môže byť mimoriadne intenzívne z toho dôvodu, že pri vyhľadávaní prostredníctvom mena dochádza ku zhromaždeniu všetkých informácií týkajúcich sa dotknutej osoby, ktoré sa nachádzajú na internete. V rámci tohto autonómneho posúdenia treba zohľadniť skutočnosť, že toto zobrazenie predstavuje samo osebe výsledok, ktorý používateľ internetu hľadá, a to bez ohľadu na jeho následné rozhodnutie navštíviť či nenavštíviť pôvodnú internetovú stránku.

Súdny dvor však poznamenal, že takéto špecifické zváženie, ktoré zohľadňuje autonómnu povahu spracúvania, ktoré uskutočňuje poskytovateľ vyhľadávača, nemá vplyv na prípadnú relevantnosť textových prvkov, ktoré môžu byť priamo pripojené k zobrazeniu fotografie v zozname výsledkov vyhľadávania, keďže takéto prvky sú spôsobilé objasniť informačnú hodnotu tejto fotografie pre verejnosť, a teda mať vplyv na vyváženie práv a záujmov, o aké ide.

4. Súhlas používateľa internetovej stránky s uchovávaním informácií

Rozsudok z 1. októbra 2019 (veľká komora), Planet49 (C-673/17, EU:C:2019:801)

V tomto rozsudku Súdny dvor rozhodol, že súhlas s uchovávaním informácií alebo prístupom k informáciám prostredníctvom súborov cookies umiestnených na koncovom zariadení používateľa internetovej stránky nie je platne daný, ak povolenie vyplýva z vopred označeného políčka, a to bez ohľadu na to, či predmetné informácie predstavujú osobné údaje. Súdny dvor navyše spresnil, že poskytovateľ služieb musí používateľovi internetovej stránky oznámiť dĺžku funkčnosti cookies, ako aj to, či tretie osoby majú alebo nemajú prístup k týmto cookies.

Spor vo veci samej sa týkal organizovania výhernej hry spoločnosťou Planet49 na internetovej stránke www.dein-macbook.de. S cieľom zúčastniť sa na tejto hre museli používatelia internetu uviesť svoje meno a adresu na webovej stránke, na ktorej sa nachádzali začiarkavacie políčka. Začiarkavacie políčko povoľujúce ukladanie cookies bolo vopred označené. Bundesgerichtshof (Spolkový súdny dvor, Nemecko), na ktorý sa obrátil nemecký Zväz spotrebiteľských združení, mal pochybnosti o platnosti získania súhlasu používateľov prostredníctvom vopred označeného začiarkavacieho políčka, ako aj o rozsahu informačnej povinnosti, ktorú má poskytovateľ služieb.

Návrh na začatie prejudiciálneho konania sa v podstate týka výkladu pojmu „súhlas“, na ktorý sa vzťahuje smernica 2002/58[94], v spojení so smernicou 95/46/ES[95], ako aj s GDPR[96].

[94] Článok 2 písm. f) a článok 5 ods. 3 smernice 2002/58, zmenenej smernicou Európskeho parlamentu a Rady 2009/136/ES z 25. novembra 2009 (Ú. v. EÚ L 337, 2009, s. 11).
[95] Článok 2 písm. h) smernice 95/46.
[96] Článok 6 ods. 1 písm. a) nariadenia 2016/679.

Po prvé Súdny dvor uviedol, že článok 2 písm. h) smernice 95/46/ES, na ktorú odkazuje článok 2 písm. f) smernice 2002/58, definuje súhlas ako akýkoľvek slobodne daný, konkrétny a informovaný prejav vôle dotknutej osoby, ktorým vyjadruje súhlas so spracúvaním osobných údajov, ktoré sa jej týka. Podľa neho požiadavka „prejavu“ vôle dotknutej osoby jasne poukazuje na aktívne a nie pasívne správanie. Súhlas daný prostredníctvom vopred označeného začiarkavacieho políčka, ktorého označenie musí používateľ zrušiť, si však nevyžaduje aktívne správanie používateľa internetovej stránky. Okrem toho genéza článku 5 ods. 3 smernice 2002/58, ktorá od svojej zmeny smernicou 2009/136 vyžaduje, aby používateľ „dal súhlas“ s ukladaním cookies, tak naznačuje, že súhlas používateľa už nemožno predpokladať a musí vyplývať z jeho aktívneho správania. Napokon, aktívny súhlas je teraz už upravený v GDPR[97], ktorého článok 4 bod 11 si vyžaduje prejav vôle, ktorý má najmä podobu „jednoznačného potvrdzujúceho úkonu“ a ktorého odôvodnenie 32 výslovne vylučuje, aby sa za súhlas považovalo „mlčanie, vopred označené políčka alebo nečinnosť“.

Súdny dvor preto rozhodol, že súhlas nie je účinne daný vtedy, keď je ukladanie informácií v koncovom zariadení používateľa internetovej stránky alebo pristupovanie k informáciám, ktoré sú tam už uložené, povolené vopred označeným začiarkavacím políčkom, ktorého označenie musí používateľ zrušiť, aby odmietol dať svoj súhlas. Súdny dvor dodal, že skutočnosť, že používateľ klikne na dotknuté tlačidlo zúčastnenia sa na výhernej hre, nemôže teda stačiť na vyvodenie záveru, že účinne dal svoj súhlas s ukladaním cookies.

Po druhé Súdny dvor konštatoval, že cieľom článku 5 ods. 3 smernice 2002/58 je chrániť používateľov pred zásahmi do ich súkromia bez ohľadu na to, či sa tento zásah týka alebo netýka osobných údajov. Z toho vyplýva, že pojem „súhlas“ sa nemá vykladať odlišne podľa toho, či informácie uložené v koncovom zariadení používateľa internetovej stránky alebo informácie, do ktorých sa v takom zariadení nahliada, predstavujú alebo nepredstavujú osobné údaje.

Po tretie Súdny dvor uviedol, že článok 5 ods. 3 smernice 2002/58 vyžaduje, aby používateľ dal vopred svoj súhlas na základe jasných a komplexných informácií, najmä o účeloch spracúvania. Jasné a komplexné informácie pritom musia používateľovi umožniť jednoducho určiť následky súhlasu, ktorý môže poskytnúť, a zabezpečiť, že bude poskytnutý informovaný súhlas. V tejto súvislosti Súdny dvor konštatoval, že dĺžka funkčnosti cookies, ako aj možnosť alebo nemožnosť tretích osôb mať prístup k týmto cookies, sú súčasťou jasných a komplexných informácií, ktoré musia byť poskytnuté používateľovi internetovej stránky poskytovateľom služieb.

[97] TAMŽE.

5. Spracúvanie osobných údajov na online sociálnych sieťach

Rozsudok zo 4. júla 2023 (veľká komora), Meta Platforms a i. (Všeobecné podmienky používania sociálnej siete) (C-252/21, EU:C:2023:537)

Spoločnosť Meta Platforms je vlastníkom online sociálnej siete „Facebook“, ktorá je pre súkromných používateľov bezplatná. Obchodný model tejto sociálnej siete je založený na financovaní prostredníctvom online reklamy, ktorá je prispôsobená jej jednotlivým používateľom. Technickým základom takejto reklamy je automatizované zostavovanie detailných profilov používateľov siete a online služieb ponúkaných na úrovni skupiny Meta. Na to, aby používatelia mohli používať uvedenú sociálnu sieť, musia v čase svojho zápisu súhlasiť so všeobecnými podmienkami vypracovanými spoločnosťou Meta Platforms, ktoré odkazujú na zásady používania údajov a súborov cookies stanovené touto spoločnosťou. Podľa týchto všeobecných podmienok Meta Platforms Ireland zhromažďuje okrem údajov, ktoré títo používatelia zadávajú priamo pri ich registrácii, aj údaje týkajúce sa aktivít uvedených používateľov na sociálnej sieti aj mimo nej, a priraďuje ich k účtom dotknutých používateľov na Facebooku. Pokiaľ ide o posledné uvedené údaje, označované tiež ako „údaje *off* Facebook“, ide jednak o údaje týkajúce sa navštevovania internetových stránok a aplikácií tretích strán a jednak o údaje o používaní iných online služieb patriacich do skupiny Meta (medzi ktoré patrí Instagram a WhatsApp). Takto zhromaždené údaje umožňujú ako celok vyvodiť podrobné závery o preferenciách a záujmoch týchto používateľov.

Rozhodnutím zo 6. februára 2019 Bundeskartellamt (Spolkový úrad pre hospodársku súťaž, Nemecko) zakázal spoločnosti Meta Platforms, aby vo všeobecných podmienkach, ktoré boli v tom čase platné, podmienila používanie sociálnej siete Facebook súkromnými používateľmi s bydliskom v Nemecku spracúvaním ich údajov off Facebook a aby bez ich súhlasu spracúvala tieto údaje. Okrem toho jej Spolkový úrad pre hospodársku súťaž uložil povinnosť, aby tieto všeobecné podmienky upravila tak, aby z nich jasne vyplývalo, že uvedené údaje sa nebudú zhromažďovať, prepájať s používateľskými účtami na Facebooku ani používať bez súhlasu dotknutých používateľov. Napokon tento úrad zdôraznil, že takýto súhlas nie je platný, ak predstavuje podmienku pre používanie sociálnej siete. Svoje rozhodnutie odôvodnil tým, že spracúvanie predmetných údajov, ktoré nie je v súlade s GDPR, predstavuje zneužívanie dominantného postavenia spoločnosti Meta Platforms na trhu online sociálnych sietí.

Meta Platforms podala proti tomuto rozhodnutiu žalobu na Oberlandesgericht Düsseldorf (Vyšší krajinský súd Düsseldorf, Nemecko). Keďže tento súd mal predovšetkým pochybnosti v súvislosti s výkladom a uplatňovaním niektorých ustanovení GDPR, obrátil sa na Súdny dvor s návrhom na začatie prejudiciálneho konania.

Súdny dvor zasadajúci vo veľkej komore vo svojom rozsudku poskytol spresnenia k možnosti prevádzkovateľa sociálnej site spracúvať „citlivé“ osobné údaje jej používateľov, k podmienkam, za ktorých je spracúvanie údajov takýmto prevádzkovateľom zákonné, ako aj k platnosti súhlasu, ktorý na účely takéhoto spracúvania udelili títo používatelia podniku s dominantným postavením na vnútroštátnom trhu online sociálnych sietí.

Pokiaľ ide o spracúvanie osobitných kategórií osobných údajov,[98] Súdny dvor zastával názor, že v prípade, ak používateľ online sociálnej siete navštívi internetové stránky alebo aplikácie majúce vzťah k jednej alebo k viacerým týmto kategóriám a prípadne do nich zadá údaje prostredníctvom registrácie alebo uskutočnenia online objednávok, treba spracúvanie osobných údajov prevádzkovateľom tejto online sociálnej siete[99] považovať za „spracúvanie osobitných kategórií osobných údajov“ v zmysle článku 9 ods. 1 GDPR, ak môže odhaliť informácie patriace do jednej z týchto osobitných kategórií, bez ohľadu na to, či sa tieto informácie týkajú používateľa tejto siete alebo akejkoľvek inej fyzickej osoby. Takéto spracúvanie údajov je s výhradou určitých výnimiek v zásade zakázané.[100]

V poslednej uvedenej súvislosti Súdny dvor spresnil, že ak používateľ online sociálnej siete navštívi internetové stránky alebo aplikácie, ktoré súvisia s jednou alebo viacerými uvedenými osobitnými kategóriami údajov, zjavne nezverejňuje[101] údaje týkajúce sa tohto navštívenia, ktoré zhromaždil prevádzkovateľ tejto online sociálnej siete prostredníctvom súborov cookies alebo podobných technológií ukladania údajov. Okrem toho, ak takýto používateľ zadá údaje na takýchto internetových stránkach, resp. v takýchto aplikáciách, alebo klikne na tlačidlá výberu na týchto stránkach alebo v týchto aplikáciách, akými sú tlačidlá „Páči sa mi to“ alebo „Zdieľať“ alebo tlačidlá umožňujúce používateľovi identifikovať sa na týchto stránkach alebo v týchto aplikáciách pomocou prihlasovacích údajov spojených s jeho používateľským účtom na sociálnej sieti, jeho telefónnym číslom alebo e-mailovou adresou, zjavne zverejňuje takto zadané údaje alebo údaje vyplývajúce z kliknutia na tieto tlačidlá len v prípade, že vopred výslovne vyjadril svoju voľbu, prípadne na základe individuálneho nastavenia vykonaného s úplnou znalosťou veci, zverejniť údaje, ktoré sa ho týkajú, neobmedzenému počtu osôb.

---

98 Uvedené v článku 9 ods. 1 GDPR. Toto ustanovenie stanovuje, že „zakazuje sa spracúvanie osobných údajov, ktoré odhaľujú rasový alebo etnický pôvod, politické názory, náboženské alebo filozofické presvedčenie alebo členstvo v odborových organizáciách, a spracúvanie genetických údajov, biometrických údajov na individuálnu identifikáciu fyzickej osoby, údajov týkajúcich sa zdravia alebo údajov týkajúcich sa sexuálneho života alebo sexuálnej orientácie fyzickej osoby“.

99 Toto spracúvanie spočíva v zhromažďovaní údajov získaných z prehliadania týchto stránok a aplikácií, ako aj údajov zadaných používateľom, a to prostredníctvom integrovaných rozhraní, súborov cookies alebo podobných technológií ukladania údajov, v prepájaní všetkých týchto údajov s účtom používateľa na sociálnej sieti a v ich používaní týmto prevádzkovateľom.

100 Stanovených v článku 9 ods. 2 GDPR. V tomto ustanovení sa uvádza: „Odsek 1 sa neuplatňuje, ak platí niektorá z týchto podmienok:
a) dotknutá osoba vyjadrila výslovný súhlas so spracúvaním týchto osobných údajov na jeden alebo viacero určených účelov, s výnimkou prípadov, keď sa v práve Únie alebo v práve členského štátu stanovuje, že zákaz uvedený v odseku 1 nemôže dotknutá osoba zrušiť;...
e) spracúvanie sa týka osobných údajov, ktoré dotknutá osoba preukázateľne zverejnila;
f) spracúvanie je nevyhnutné na preukazovanie, uplatňovanie alebo obhajovanie právnych nárokov, alebo kedykoľvek, keď súdy vykonávajú svoju súdnu právomoc;...“

101 V zmysle článku 9 ods. 2 písm. e) GDPR.

Pokiaľ ide všeobecne o podmienky zákonnosti spracúvania osobných údajov, Súdny dvor pripomenul, že podľa GDPR je spracúvanie osobných údajov zákonné iba vtedy a iba rozsahu, v akom s ním dotknutá osoba súhlasila na jeden alebo viacero konkrétnych účelov.[102] V prípade neexistencie takéhoto súhlasu alebo v prípade, že tento súhlas nebol daný slobodne, konkrétne, informovaným a jednoznačným spôsobom, je takéto spracúvanie napriek tomu odôvodnené, ak spĺňa niektorú z požiadaviek nevyhnutnosti[103], ktoré sa musia vykladať reštriktívne. Spracúvanie osobných údajov používateľov uskutočnené prevádzkovateľom online sociálnej siete však možno považovať za nevyhnutné na plnenie zmluvy, ktorej zmluvnými stranami sú títo používatelia, len pod podmienkou, že toto spracúvanie je objektívne nevyhnutné na dosiahnutie cieľa, ktorý je neoddeliteľnou súčasťou zmluvného plnenia určeného uvedeným používateľom, takže bez tohto spracúvania by nebolo možné dosiahnuť hlavný predmet zmluvy.

Navyše podľa Súdneho dvora možno predmetné spracúvanie považovať za nevyhnutné na účely oprávnených záujmov, ktoré sleduje prevádzkovateľ alebo tretia strana, len pod podmienkou, že uvedený prevádzkovateľ oznámil používateľom, od ktorých boli údaje získané, oprávnený záujem, ktorý sa ich spracúvaním sleduje, že toto spracúvanie sa uskutočňuje v medziach toho, čo je nevyhnutne potrebné na dosiahnutie tohto oprávneného záujmu, a že so zreteľom na všetky relevantné okolnosti zo zváženia protichodných záujmov vyplýva, že záujmy alebo základné práva a slobody týchto používateľov neprevažujú nad uvedeným oprávneným záujmom prevádzkovateľa alebo tretej strany. Súdny dvor sa pritom najmä domnieval, že bez ich súhlasu prevažujú záujmy a základné práva uvedených používateľov nad záujmom prevádzkovateľa online sociálnej siete na personalizácii reklamy, prostredníctvom ktorej financuje svoju činnosť.

Napokon Súdny dvor spresnil, že predmetné spracúvanie údajov je odôvodnené, ak je skutočne nevyhnutné na splnenie zákonnej povinnosti, ktorá sa vzťahuje na prevádzkovateľa na základe ustanovenia práva Únie alebo práva dotknutého členského štátu, že tento právny základ zodpovedá cieľu verejného záujmu a je primeraný sledovanému legitímnemu cieľu a že toto spracúvanie sa uskutočňuje v medziach toho, čo je nevyhnutne potrebné.

Pokiaľ ide o platnosť súhlasu dotknutých používateľov so spracúvaním ich údajov na základe GDPR, Súdny dvor sa domnieval, že okolnosť, že prevádzkovateľ online sociálnej siete má dominantné postavenie na trhu s online sociálnymi sieťami, sama osebe nebráni tomu, aby používatelia takejto siete mohli platne udeliť súhlas so spracúvaním svojich osobných údajov týmto prevádzkovateľom. Vzhľadom na to, že takéto postavenie môže ovplyvniť slobodu voľby týchto používateľov a spôsobiť zjavnú nerovnováhu medzi týmito používateľmi a uvedeným prevádzkovateľom, je však táto okolnosť dôležitým

[102] Podľa článku 6 ods. 1 prvého pododseku písm. a) GDPR.

[103] Uvedené v článku 6 ods. 1 prvom pododseku písm. b) až f) GDPR. Podľa týchto ustanovení je spracúvanie zákonné iba vtedy a iba rozsahu, v akom je okrem iného nevyhnutné na plnenie zmluvy, ktorej zmluvnou stranou je dotknutá osoba [článok 6 ods. 1 prvý pododsek písm. b) GDPR], na splnenie zákonnej povinnosti prevádzkovateľa [článok 6 ods. 1 prvý pododsek písm. c) GDPR] alebo na účely oprávnených záujmov, ktoré sleduje prevádzkovateľ alebo tretia strana [článok 6 ods. 1 prvý pododsek písm. f) GDPR].

prvkom pri určení, či bol súhlas skutočne poskytnutý platne, a najmä slobodne, čo musí preukázať tento prevádzkovateľ[104].

Konkrétne používatelia predmetných sociálnych sietí musia mať v rámci zmluvného procesu možnosť individuálne odmietnuť udeliť svoj súhlas s konkrétnymi operáciami spracúvania údajov, ktoré nie sú nevyhnutné na plnenie zmluvy, bez toho, aby boli povinní sa v plnom rozsahu vzdať používania tejto online sociálnej siete, čo znamená, že uvedeným používateľom sa ponúkne, prípadne za primeranú odmenu, rovnocenná alternatíva, s ktorou nie sú spojené takéto operácie spracúvania údajov. Navyše musí byť možné udeliť samostatný súhlas so spracúvaním údajov off Facebook.

VI. Vnútroštátne dozorné orgány

1. Rozsah požiadavky nezávislosti

Rozsudok z 9. marca 2010 (veľká komora), Komisia/Nemecko (C-518/07, EU:C:2010:125)

Komisia vo svojej žalobe navrhovala, aby Súdny dvor určil, že Spolková republika Nemecko si tým, že podriadila štátnemu dohľadu dozorné orgány poverené dohľadom nad spracovaním osobných údajov v neverejnom sektore v rôznych spolkových krajinách, čím nesprávne prebrala požiadavku „úplnej nezávislosti“ orgánov poverených zabezpečením ochrany týchto údajov, nesplnila povinnosti, ktoré jej vyplývajú z článku 28 ods. 1 druhého pododseku smernice 95/46.

Spolková republika Nemecko sa domnievala, že článok 28 ods. 1 druhý pododsek smernice 95/46 vyžaduje funkčnú nezávislosť dozorných orgánov v tom zmysle, že tieto orgány musia byť nezávislé od neverejného sektora podliehajúceho ich kontrole a nesmú byť vystavené vonkajším vplyvom. Podľa jej názoru pritom štátny dohľad vykonávaný v spolkových krajinách v Nemecku nepredstavuje takýto vonkajší vplyv, ale predstavuje mechanizmus vnútorného dohľadu nad administratívou vykonávaný prostredníctvom správnych orgánov, ktoré patria do rovnakého správneho aparátu ako dozorné orgány a musia rovnako ako tieto orgány plniť ciele smernice 95/46.

Súdny dvor rozhodol, že záruka nezávislosti vnútroštátnych dozorných orgánov, stanovená v smernici 95/46, má zabezpečiť účinnosť a spoľahlivosť dohľadu nad dodržiavaním právnych predpisov v oblasti ochrany fyzických osôb pri spracovaní osobných údajov a má sa vykladať vo svetle tohto cieľa. Táto záruka nebola vytvorená preto, aby uvedeným orgánom ako takým a ich úradníkom priznala osobitné postavenie,

[104] Na základe článku 7 ods. 1 nariadenia GDPR.

ale preto, aby posilnila ochranu osôb a subjektov dotknutých ich rozhodnutiami, pričom dozorné orgány musia pri vykonávaní svojich úloh konať objektívne a nestranne.

V dôsledku toho musí byť týmto dozorným orgánom povereným dohľadom nad spracovaním osobných údajov v neverejnom sektore priznaná nezávislosť, ktorá im umožní vykonávať svoje úlohy bez vonkajšieho vplyvu. Táto nezávislosť vylučuje nielen akýkoľvek vplyv zo strany kontrolovaných subjektov, ale aj akýkoľvek príkaz a iný vonkajší vplyv, či už priamy alebo nepriamy, ktorý by mohol spochybniť to, aby uvedené orgány vykonávali úlohy, ktoré spočívajú v zabezpečení spravodlivej rovnováhy medzi ochranou základného práva na súkromie a voľným pohybom osobných údajov. Samotné riziko, že orgány štátneho dohľadu budú môcť politicky ovplyvňovať rozhodnutia príslušných dozorných orgánov, postačuje na narušenie nezávislého plnenia úloh týchto orgánov. Na jednej strane môže ísť o „predpokladanú poslušnosť“ týchto orgánov v súvislosti s rozhodovacou praxou orgánu štátneho dohľadu. Na druhej strane úloha strážcu práva na súkromie, ktorú zastávajú uvedené orgány, vyžaduje, aby boli ich rozhodnutia, ako aj samotné orgány mimo akéhokoľvek podozrenia zo zaujatosti. Podľa Súdneho dvora štátny dohľad vykonávaný nad vnútroštátnymi dozornými orgánmi teda nie je zlučiteľný s požiadavkou nezávislosti.

Rozsudok zo 16. októbra 2012 (veľká komora), Komisia/Rakúsko (C-614/10, EU:C:2012:631***)***

Svojou žalobou Komisia požiadala Súdny dvor, aby určil, že Rakúsko si tým, že neprijalo všetky právne predpisy nevyhnutné na to, aby právna úprava platná v Rakúsku spĺňala kritérium nezávislosti, pokiaľ ide o Datenschutzkommission (komisia pre ochranu údajov), zriadenú ako dozorný orgán pre ochranu osobných údajov, nesplnilo povinnosti, ktoré mu vyplývajú z článku 28 ods. 1 druhého pododseku smernice 95/46.

Súdny dvor konštatoval nesplnenie si povinnosti zo strany Rakúska, pričom v podstate usúdil, že členský štát, ktorý zavedie regulačný rámec, podľa ktorého je správca uvedeného orgánu štátnym úradníkom podliehajúcim služobnému dohľadu, ktorého kancelária je začlenená medzi útvary národnej vlády a vo vzťahu ku ktorému má predseda národnej vlády bezpodmienečné právo na informácie týkajúce sa všetkých aspektov riadenia uvedeného orgánu, nespĺňa kritérium nezávislosti dozorného orgánu, ktoré stanovuje smernica 95/46.

Súdny dvor najskôr pripomenul, že výraz „s úplnou nezávislosťou“ uvedený v článku 28 ods. 1 druhom pododseku smernice 95/46 znamená, že dozorným orgánom sa musí priznať nezávislosť, ktorá im umožní vykonávať ich úlohy bez vonkajšieho vplyvu. V tomto ohľade skutočnosť, že takýto orgán má funkčnú nezávislosť, lebo jeho členovia sú nezávislí a pri výkone svojej funkcie nie sú viazaní nijakými pokynmi, sama osebe nepostačuje na to, aby uvedený dozorný orgán uchránila od akéhokoľvek vonkajšieho vplyvu. Cieľom nezávislosti požadovanej v tomto rámci je pritom nielen vylúčiť priamy vplyv vo forme pokynov, ale takisto akúkoľvek formu nepriameho vplyvu, ktorý by mohol usmerňovať rozhodnutia dozorného orgánu. Navyše vzhľadom na úlohu strážcu práva

na súkromie, ktorú si plnia uvedené orgány, je potrebné, aby ich rozhodnutia, ako aj samotné orgány boli mimo akéhokoľvek podozrenia zo zaujatosti.

Súdny dvor spresnil, že na to, aby vnútroštátny dozorný orgán spĺňal kritérium nezávislosti uvedené v už citovanom ustanovení smernice 95/46, tento orgán nemusí mať k dispozícii samostatnú rozpočtovú položku, ako je to v prípade rozpočtovej položky upravenej v článku 43 ods. 3 nariadenia č. 45/2001. Členské štáty totiž nie sú povinné prevziať do svojich vnútroštátnych právnych predpisov ustanovenia obdobné ustanoveniam kapitoly V nariadenia č. 45/2001, aby sa zaručila úplná nezávislosť ich dozorných orgánov, a môžu teda stanoviť, že z hľadiska rozpočtového práva je dozorný orgán závislý od určitého ministerského odboru. Poskytnutie ľudských a materiálnych prostriedkov, ktoré sú pre takýto orgán nevyhnutné, mu však nesmie brániť vo vykonávaní jeho funkcií „s úplnou nezávislosťou“ v zmysle článku 28 ods. 1 druhého pododseku smernice 95/46.

Rozsudok z 8. apríla 2014 (veľká komora), Komisia/Maďarsko (C-288/12, EU:C:2014:237)

V tejto veci Komisia navrhla, aby Súdny dvor konštatoval, že Maďarsko si predčasným ukončením funkčného obdobia dozorného orgánu pre ochranu osobných údajov nesplnilo povinnosti, ktoré mu vyplývajú zo smernice 95/46.

Súdny dvor rozhodol, že členský štát, ktorý predčasne ukončí funkčné obdobie dozorného orgánu pre ochranu osobných údajov, si neplní povinnosti, ktoré mu vyplývajú zo smernice 95/46.

Podľa Súdneho dvora nezávislosť, ktorá musí byť priznaná dozorným orgánom povereným dohľadom nad spracovaním uvedených údajov, totiž vylučuje najmä akýkoľvek príkaz či iný vonkajší vplyv v akejkoľvek forme, či už priamy alebo nepriamy, ktorý by mohol ovplyvniť ich rozhodnutia a tým spochybniť vykonávanie úloh uvedenými orgánmi, ktoré spočívajú v zabezpečení spravodlivej rovnováhy medzi ochranou základného práva na súkromie a voľným pohybom osobných údajov.

Súdny dvor okrem iného pripomenul, že keďže funkčná nezávislosť sama osebe nepostačuje na to, aby dozorné orgány uchránila od akéhokoľvek vonkajšieho vplyvu, samotné riziko, že orgány štátneho dohľadu budú môcť politicky ovplyvňovať rozhodnutia dozorných orgánov, postačuje na narušenie nezávislého plnenia úloh týchto orgánov. Keby každý členský štát mohol ukončiť funkčné obdobie dozorného orgánu pred ukončením jeho vopred určenej dĺžky bez toho, aby rešpektoval pravidlá a záruky stanovené na tieto účely uplatniteľnou právnou úpravou, hrozba takéhoto predčasného ukončenia, ktorej by tento orgán musel čeliť počas celého svojho funkčného obdobia, by mohla viesť k určitej forme poslušnosti tohto orgánu voči politickej moci, ktorá je s uvedenou požiadavkou nezávislosti nezlučiteľná. Navyše v takejto situácii by nebolo možné predpokladať, že dozorný orgán môže za každých okolností konať mimo akéhokoľvek podozrenia zo zaujatosti.

2. Určenie uplatniteľného práva a príslušného dozorného orgánu

Rozsudok z 1. októbra 2015, Weltimmo (C-230/14, EU:C:2015:639)

Nemzeti Adatvédelmi és Információszabadság Hatóság (Národný úrad na ochranu údajov a slobodu informácií, Maďarsko) uložil spoločnosti Weltimmo, registrovanej na Slovensku, ktorá prevádzkuje internetové stránky s inzerátmi na nehnuteľnosti nachádzajúce sa v Maďarsku, pokutu z dôvodu, že z týchto stránok nevymazala osobné údaje inzerentov napriek ich žiadosti v tomto zmysle a oznámila tieto údaje spoločnostiam zaoberajúcim sa vymáhaním pohľadávok, aby dosiahla úhradu nezaplatených faktúr. Podľa maďarského dozorného orgánu tak Weltimmo porušila maďarský zákon, ktorým sa preberá smernica 95/46.

Kúria (Najvyšší súd, Maďarsko), rozhodujúci o kasačnom opravnom prostriedku, vyjadril pochybnosti, pokiaľ ide o určenie uplatniteľného práva a o právomoci maďarského kontrolného orgánu s ohľadom na článok 4 ods. 1 a článok 28 smernice 95/46. V dôsledku toho položil Súdnemu dvoru viacero prejudiciálnych otázok.

Pokiaľ ide o uplatniteľné vnútroštátne právo, Súdny dvor rozhodol, že článok 4 ods. 1 písm. a) smernice 95/46 umožňuje uplatnenie právnej úpravy týkajúcej sa ochrany osobných údajov iného členského štátu, ako je členský štát, v ktorom je prevádzkovateľ spracúvajúci tieto údaje zapísaný, pokiaľ tento prevádzkovateľ na území prvého členského štátu vykonáva prostredníctvom stálej prevádzkarne hoci aj minimálnu skutočnú a efektívnu činnosť, v rámci ktorej sa toto spracúvanie vykonáva. Na účely určenia, či je to tak, môže vnútroštátny súd na jednej strane zohľadniť najmä skutočnosť, že činnosť prevádzkovateľa spracúvajúceho údaje, v kontexte ktorej sa toto spracovanie vykonáva, spočíva v prevádzkovaní internetových stránok s inzerátmi na nehnuteľnosti, ktoré sa nachádzajú na území tohto členského štátu, v jazyku tohto štátu, a že teda prevažne, či dokonca úplne smeruje do uvedeného členského štátu. Vnútroštátny súd môže na druhej strane tiež zohľadniť skutočnosť, že tento prevádzkovateľ má v uvedenom členskom štáte zástupcu, ktorý je poverený vymáhaním pohľadávok vyplývajúcich z tejto činnosti, ako aj zastupovaním prevádzkovateľa v správnych a súdnych konaniach týkajúcich sa spracovania dotknutých údajov. Súdny dvor naproti tomu spresnil, že otázka štátnej príslušnosti osôb dotknutých týmto spracovaním údajov nie je relevantná.

Pokiaľ ide o príslušnosť a právomoci dozorného orgánu, ktorý začal konať v súlade s článkom 28 ods. 4 smernice 95/46, Súdny dvor usúdil, že tento orgán môže preskúmať tieto sťažnosti bez ohľadu na uplatniteľné právo a dokonca ešte pred zistením, ktoré vnútroštátne právo je na dotknuté spracovanie údajov uplatniteľné. Ak však dôjde k záveru, že uplatniteľné je právo iného členského štátu, nemôže ukladať sankcie mimo územia svojho členského štátu. V takejto situácii musí v súlade s povinnosťou spolupráce uloženou článkom 28 ods. 6 tejto smernice požiadať dozorný orgán tohto iného členského štátu, aby rozhodol o prípadnom porušení tohto práva a uložil sankcie, ak to

uvedené právo dovoľuje, pričom sa môže prípadne opierať o informácie, ktoré mu poskytol dozorný orgán prvého členského štátu.

3. Právomoci vnútroštátnych dozorných orgánov

Rozsudok zo 6. októbra 2015 (veľká komora), Schrems (C-362/14, EU:C:2015:650)

V tejto veci (pozri tiež rubriku IV s názvom „Prenos osobných údajov do tretích krajín“) Súdny dvor najmä rozhodol, že vnútroštátne dozorné orgány majú právomoc vykonávať dohľad nad prenosom osobných údajov do tretích krajín.

Súdny dvor v tejto súvislosti predovšetkým konštatoval, že vnútroštátne dozorné orgány disponujú veľkým rozsahom právomocí a tieto právomoci, ktoré sú demonštratívne vymenované v článku 28 ods. 3 smernice 95/46, predstavujú nevyhnutné prostriedky na vykonávanie ich povinností. Tieto orgány majú najmä vyšetrovacie právomoci, ako je právo zbierať všetky nevyhnutné informácie pre plnenie ich kontrolných povinností, efektívne právomoci intervencie, ako je napríklad uvalenie dočasného alebo úplného zákazu na spracovanie údajov, alebo tiež právomoc obrátiť sa na súdne orgány.

Pokiaľ ide o právomoc kontrolovať prenosy osobných údajov do tretích krajín, Súdny dvor rozhodol, že z článku 28 ods. 1 a 6 smernice 95/46 nepochybne vyplýva, že právomoci vnútroštátnych dozorných orgánov sa týkajú spracovania osobných údajov vykonaných na území členského štátu, ktorému tieto orgány podliehajú, takže nemajú právomoci na základe tohto článku 28 vo vzťahu k spracovaniu takýchto údajov vykonanému na území tretej krajiny.

Činnosť spočívajúca v prenose osobných údajov z členského štátu do tretej krajiny však sama osebe predstavuje spracovanie osobných údajov vykonané na území členského štátu. V dôsledku toho, keďže vnútroštátne dozorné orgány sú v súlade s článkom 8 ods. 3 Charty a s článkom 28 smernice 95/46 poverené kontrolou dodržiavania pravidiel Únie o ochrane fyzických osôb pri spracovaní osobných údajov, každý z nich má právomoc overiť, či prenos osobných údajov z členského štátu, ktorému podlieha, do tretej krajiny spĺňa požiadavky stanovené touto smernicou.

Rozsudok z 5. júna 2018 (veľká komora), Wirtschaftsakademie Schleswig-Holstein (C-210/16, EU:C:2018:388)

V tomto rozsudku (pozri tiež rubriku II.5. s názvom „Pojem ‚prevádzkovateľ spracovania osobných údajov‘“), ktorý sa okrem iného týka výkladu článkov 4 a 28 smernice 95/46, Súdny dvor rozhodol o rozsahu intervenčných právomocí dozorných orgánov v súvislosti so spracovaním osobných údajov, ktoré zahŕňa účasť viacerých subjektov.

Súdny dvor tak rozhodol, že pokiaľ má podnik so sídlom mimo Európskej únie (akým je americká spoločnosť Facebook) niekoľko prevádzkarní v rôznych členských štátoch, dozorný orgán členského štátu je oprávnený vykonávať právomoci, ktoré mu zveruje článok 28 ods. 3 tejto smernice, voči prevádzkarni tohto podniku nachádzajúcej sa na území tohto členského štátu (v tomto prípade Facebook Germany), hoci na jednej strane na základe rozdelenia úloh v rámci skupiny je táto prevádzkareň zodpovedná len za predaj reklamných priestorov a iné marketingové činnosti na území uvedeného členského štátu a na druhej strane výlučnú zodpovednosť za zber a spracovanie osobných údajov na celom území Európskej únie má prevádzkareň, ktorá sa nachádza v inom členskom štáte (v tomto prípade Facebook Ireland).

Súdny dvor navyše spresnil, že keď má dozorný orgán jedného členského štátu v úmysle vykonať voči subjektu usadenému na území tohto členského štátu intervenčné právomoci uvedené v článku 28 ods. 3 smernice 95/46 z dôvodu porušenia pravidiel týkajúcich sa ochrany osobných údajov, ktorých sa dopustila tretia osoba zodpovedná za spracovanie týchto údajov, ktorá má svoje sídlo v inom členskom štáte (v tejto veci spoločnosť Facebook Ireland), je tento dozorný orgán oprávnený nezávisle od dozorného orgánu tohto posledného uvedeného členského štátu (Írsko) posúdiť zákonnosť takéhoto spracovania údajov a môže vykonávať svoje intervenčné právomoci voči subjektu usadenému na svojom území bez toho, aby predtým požiadal dozorný orgán iného členského štátu, aby zasiahol.

Rozsudok z 15. júna 2021 (veľká komora), Facebook Ireland a i. (C-645/19, EU:C:2021:483)

Dňa 11. septembra 2015 podal predseda belgickej Komisie na ochranu súkromia (ďalej len „CBPL“) na Nederlandstalige rechtbank van eerste aanleg Brussel (Holandskojazyčný súd prvého stupňa v Bruseli, Belgicko) návrh na zdržanie sa konania proti spoločnostiam Facebook Ireland, Facebook Inc. a Facebook Belgium, ktorým sa domáhal skončenia údajného porušovania právnych predpisov o ochrane údajov zo strany spoločnosti Facebook. Tieto porušenia spočívali najmä v získavaní a používaní informácií o správaní belgických používateľov internetu, ktorí mali účet na Facebooku, ako aj tých, ktorý taký účet nemali, pri surfovaní, a to rôznymi technológiami, ako sú súbory cookies, moduly sociálnych sietí[105] alebo technológiou pixels.

Dňa 16. februára 2018 tento súd vyhlásil, že má právomoc rozhodovať o tejto žalobe, a pokiaľ ide o meritum veci, rozhodol, že sociálna sieť Facebook dostatočne neinformovala belgických používateľov internetu o zbieraní dotknutých informácií a ich použití. Okrem toho rozhodol, že súhlas daný používateľmi internetu so zbieraním a spracúvaním týchto informácií bol neplatný.

Dňa 2. marca 2018 Facebook Ireland, Facebook Inc. a Facebook Belgium podali proti tomuto rozsudku odvolanie na Hof van beroep te Brussel (Odvolací súd Brusel,

[105] Napríklad tlačidlá „Páči sa mi to“ alebo „Zdieľať“.

Belgicko), t. j. vnútroštátny súd v prejednávanej veci. Pred týmto súdom Úrad na ochranu osobných údajov (Belgicko) (ďalej len „GBA“) koná ako právny nástupca predsedu CBPL. Vnútroštátny súd rozhodol, že má právomoc rozhodovať o odvolaní podanom len spoločnosťou Facebook Belgium.

Vnútroštátny súd mal pochybnosti o vplyve uplatnenia mechanizmu „jednotného kontaktného miesta“ stanoveného v GDPR[106] na právomoci GBA a presnejšie sa pýtal na to, či v súvislosti so skutkovými okolnosťami po nadobudnutí účinnosti GDPR, t. j. po 25. máji 2018, môže GBA podať žalobu proti spoločnosti Facebook Belgium, vzhľadom na to, že ako prevádzkovateľ spracúvania dotknutých údajov bola identifikovaná Facebook Ireland. Od tohto dátumu a najmä na základe zásady „jednotného kontaktného miesta“ stanovenej v GDPR právomoc podať žalobu o zdržanie sa konania totiž má len írsky komisár pre ochranu údajov pod dohľadom írskych súdov.

Súdny dvor vo svojom rozsudku vyhlásenom veľkou komorou spresnil právomoci vnútroštátnych dozorných orgánov v rámci GDPR. Rozhodol najmä, že toto nariadenie oprávňuje za určitých podmienok dozorný orgán členského štátu vykonávať svoju právomoc, ktorou je upozorniť súd tohto členského štátu na akékoľvek údajné porušenie GDPR a začať súdne konanie v súvislosti s cezhraničným spracúvaním údajov,[107] hoci nie je vedúcim dozorným orgánom pre toto spracúvanie.

Po prvé Súdny dvor spresnil podmienky, za akých vnútroštátny dozorný orgán, ktorý nemá postavenie vedúceho orgánu, pokiaľ ide o cezhraničné spracúvanie, musí vykonávať svoju právomoc, ktorou je upozorniť súd členského štátu na akékoľvek údajné porušenie GDPR a prípadne začať súdne konanie na účely zabezpečenia uplatňovania tohto nariadenia. Podľa GDPR sa teda tomuto dozornému orgánu jednak musí priznávať právomoc na prijatie rozhodnutia konštatujúceho, že uvedené spracúvanie porušuje pravidlá, ktoré sú v ňom uvedené, a jednak pri výkone tejto právomoci musia byť dodržané postupy spolupráce a konzistentnosti stanovené v tomto nariadení[108].

V prípade cezhraničného spracúvania totiž GDPR stanovuje mechanizmus „jednotného kontaktného miesta“[109]založený na rozdelení právomocí medzi „vedúcim dozorným orgánom“ a inými dotknutými dozornými orgánmi. Tento mechanizmus vyžaduje úzku, lojálnu a účinnú spoluprácu medzi týmito orgánmi s cieľom zabezpečiť konzistentnú a jednotnú ochranu pravidiel týkajúcich sa ochrany osobných údajov a zachovať tak jej potrebný účinok. GDPR v tejto súvislosti zakotvuje zásadnú právomoc vedúceho dozorného orgánu prijať rozhodnutie konštatujúce, že cezhraničné zaobchádzanie porušuje pravidlá stanovené týmto nariadením,[110] zatiaľ čo právomoc ostatných vnútroštátnych dozorných orgánov prijať takéto rozhodnutie, hoci aj predbežné,

[106] Podľa článku 56 ods. 1 GDPR: „Bez toho, aby bol dotknutý článok 55, dozorný orgán hlavnej prevádzkarne alebo jedinej prevádzkarne prevádzkovateľa alebo sprostredkovateľa je príslušný konať ako vedúci dozorný orgán pre cezhraničné spracúvanie vykonávané zo strany tohto prevádzkovateľa alebo sprostredkovateľa“.
[107] V zmysle článku 4 bodu 23 GDPR.
[108] Stanovené v článkoch 56 a 60 GDPR.
[109] Článok 56 ods. 1 GDPR.
[110] Článok 60 ods. 7 GDPR.

predstavuje výnimku[111]. Vedúci dozorný orgán však nemôže pri výkone svojich právomocí upustiť od nevyhnutného dialógu, ako ani od lojálnej a účinnej spolupráce s ostatnými dotknutými dozornými orgánmi. Z tohto dôvodu vedúci dozorný orgán nemôže ignorovať názory ostatných dotknutých dozorných orgánov a každá relevantná a odôvodnená námietka niektorého z týchto orgánov má za následok aspoň dočasné zablokovanie prijatia návrhu rozhodnutia vedúceho dozorného orgánu.

Súdny dvor okrem toho spresnil, že okolnosť, že dozorný orgán členského štátu, ktorý nie je vedúcim dozorným orgánom s ohľadom na cezhraničné spracúvanie údajov, môže vykonávať právomoc upozorniť súd tohto členského štátu na akékoľvek údajné porušenie GDPR a začať súdne konanie v súvislosti s cezhraničným spracúvaním údajov len v súlade s pravidlami rozdelenia rozhodovacích právomocí medzi vedúcim dozorným orgánom a inými dozornými orgánmi[112], je v súlade s článkami 7, 8 a 47 Charty, ktoré zaručujú dotknutej osobe právo na ochranu jej osobných údajov, resp. právo na účinný prostriedok nápravy.

Po druhé Súdny dvor rozhodol, že v prípade cezhraničného spracúvania údajov výkon právomoci dozorného orgánu iného členského štátu než vedúceho dozorného orgánu podať žalobu na súde[113] nevyžaduje, aby prevádzkovateľ alebo sprostredkovateľ cezhraničného spracúvania osobných údajov, proti ktorému bola táto žaloba podaná, mal hlavnú prevádzkareň alebo inú prevádzkareň na území tohto členského štátu. Výkon tejto právomoci však musí spadať do územnej pôsobnosti GDPR[114], čo predpokladá, že prevádzkovateľ alebo sprostredkovateľ cezhraničného spracúvania má prevádzkareň na území Únie.

Po tretie Súdny dvor rozhodol, že v prípade cezhraničného spracúvania údajov je právomoc dozorného orgánu členského štátu, iného ako vedúceho dozorného orgánu, predložiť akékoľvek údajné porušenie RGPD súdu tohto štátu a prípadne môže vykonávať tak vo vzťahu k hlavnému miestu podnikania prevádzkovateľa v členskom štáte, ku ktorému tento orgán patrí, ako aj vo vzťahu k inému miestu podnikania tohto prevádzkovateľa za predpokladu, že sa súdne konanie týka spracúvania údajov vykonávaného v rámci činností tohto miesta podnikania a že tento orgán je príslušný vykonávať túto právomoc.

Súdny dvor však spresnil, že výkon tejto právomoci predpokladá, že sa GDPR uplatní. V prejednávanej veci, keďže činnosti vykonávané prevádzkarňou skupiny Facebook nachádzajúcou sa v Belgicku sú neoddeliteľne spojené so spracúvaním osobných údajov, o ktoré ide vo veci samej, za ktoré je Facebook Ireland zodpovedná vzhľadom na územie Únie, toto spracúvanie je vykonávané „v rámci činnosti prevádzk[arne] prevádzkovateľa“, a teda patrí do pôsobnosti nariadenia GDPR.

---

111 Článok 56 ods. 2 a článok 66 GDPR zakotvujú výnimky zo zásady rozhodovacej právomoci vedúceho dozorného orgánu.

112 Stanovené v článkoch 55 a 56 v spojení s článkom 60 GDPR.

113 Podľa článku 58 ods. 5 nariadenia GDPR.

114 Článok 3 ods. 1 GDPR stanovuje, že toto nariadenie sa vzťahuje na spracúvanie osobných údajov „v rámci činnosti prevádzk[arne] prevádzkovateľa alebo sprostredkovateľa v Únii, a to bez ohľadu na to, či sa spracúvanie vykonáva v Únii alebo nie“.

Po štvrté Súdny dvor rozhodol, že ak dozorný orgán členského štátu, ktorý nie je „vedúcim dozorným orgánom“, podal pred nadobudnutím účinnosti nariadenia GDPR žalobu týkajúcu sa cezhraničného spracúvania osobných údajov, v konaní o tejto žalobe sa môže podľa práva Únie pokračovať na základe ustanovení smernice 95/46, ktorá sa naďalej uplatňuje s ohľadom na porušenia v nej stanovených pravidiel, ku ktorým dochádzalo až do dátumu jej zrušenia. Okrem toho dôvodom na podanie uvedenej žaloby zo strany tohto orgánu môžu byť navyše porušenia, ku ktorým došlo po dátume nadobudnutia účinnosti GDPR, ak ide o niektorú zo situácií, pre ktoré toto nariadenie výnimočne priznáva tomuto istému dozornému orgánu právomoc na prijatie rozhodnutia konštatujúceho, že predmetné spracúvanie dotknutých údajov je v rozpore s pravidlami stanovenými v uvedenom nariadení, a pod podmienkou, že budú dodržané postupy spolupráce stanovené v tomto istom nariadení.

Po piate a napokon Súdny dvor uznal priamy účinok ustanovenia GDPR, podľa ktorého každý členský štát prostredníctvom právnych predpisov stanoví, že jeho dozorný orgán má právomoc upozorniť justičné orgány na porušenia tohto nariadenia a prípadne začať súdne konanie. V dôsledku toho sa takýto orgán môže odvolávať na toto ustanovenie s cieľom podať žalobu alebo pokračovať v konaní o žalobe, a to napriek tomu, že toto ustanovenie nebolo osobitne vykonané v právnej úprave dotknutého členského štátu.

Rozsudok zo 16. januára 2024 (veľká komora), Österreichische Datenschutzbehörde (C-33/22, EU:C:2024:46)

V tejto veci (pozri tiež rubriku II.1. s názvom „Pôsobnosť všeobecnej právnej úpravy“) Súdny dvor uviedol, že ustanovenia GDPR týkajúce sa právomoci vnútroštátnych dozorných orgánov a práva na sťažnosť[115] nevyžadujú prijatie vnútroštátnych vykonávacích opatrení a sú dostatočne jasné, presné a nepodmienené na to, aby mali priamy účinok. Z toho vyplýva, že hoci GDPR ponecháva členským štátom mieru voľnej úvahy, pokiaľ ide o počet dozorných orgánov, ktoré majú byť zriadené,[116] stanovuje rozsah ich právomocí dohliadať na uplatňovanie GDPR. V prípade, že sa členský štát rozhodne zriadiť jediný vnútroštátny dozorný orgán, má nevyhnutne všetky právomoci stanovené týmto nariadením. Akýkoľvek iný výklad by spochybnil potrebný účinok týchto ustanovení a mohol by oslabiť potrebný účinok všetkých ostatných ustanovení GDPR, ktoré môžu byť sťažnosťou dotknuté.

Pokiaľ ide o okolnosť, že vnútroštátne ustanovenia ústavnej povahy vylučujú možnosť dozorného orgánu, ktorý závisí od výkonnej moci, dohliadať na uplatňovanie GDPR orgánom patriacim do zákonodarnej moci, Súdny dvor zdôrazňuje, že práve z dôvodu rešpektovania ústavnej štruktúry členských štátov sa GDPR obmedzuje na to, že od nich vyžaduje, aby zriadili aspoň jeden dozorný orgán, pričom im poskytuje možnosť zriadiť viacero dozorných orgánov. Toto nariadenie tak priznáva každému členskému štátu

[115] Článok 55 ods. 1 a článok 77 ods. 1 GDPR.
[116] V súlade s článkom 51 ods. 1 GDPR.

určitú mieru voľnej úvahy, ktorá mu umožňuje zriadiť toľko dozorných orgánov, koľko vyžadujú najmä požiadavky súvisiace s jeho ústavnou štruktúrou.

Navyše odvolávanie sa na ustanovenia vnútroštátneho práva členským štátom nemôže ohroziť jednotu a účinnosť práva Únie. Účinky spojené so zásadou prednosti práva Únie sú totiž záväzné pre všetky orgány členského štátu, pričom tomu najmä nemôžu brániť vnútroštátne ustanovenia vrátane tých ústavných.

Ak sa teda členský štát rozhodol zriadiť jediný dozorný orgán, nemôže sa odvolávať na ustanovenia vnútroštátneho práva, a to ani v prípade, že by boli ústavnej povahy, s cieľom vyňať spracúvanie osobných údajov, ktoré patrí do pôsobnosti GDPR, z dohľadu tohto orgánu.

4. Podmienky ukladania správnych pokút

Rozsudok z 5. decembra 2023 (veľká komora), Nacionalinis visuomenės sveikatos centras (C-683/21, EU:C:2023:949)

V tejto veci (pozri tiež rubriky II.3., II.5. a II.6., nazvané „Pojem ‚spracovanie osobných údajov‘“, „Pojem ‚prevádzkovateľ spracovania osobných údajov‘“ a „Pojem ‚spoločný prevádzkovateľ spracovania osobných údajov‘“), Súdny dvor konštatoval, že podľa článku 83 GDPR možno prevádzkovateľovi uložiť správnu pokutu len vtedy, ak sa preukáže, že pravidlá obsiahnuté v tomto nariadení porušil úmyselne alebo z nedbanlivosti.[117]

V tejto súvislosti Súdny dvor spresňuje, že normotvorca Únie neponechal členským štátom mieru voľnej úvahy, pokiaľ ide o hmotnoprávne podmienky, ktoré musí dozorný orgán dodržať, keď sa rozhodne uložiť prevádzkovateľovi správnu pokutu podľa tohto ustanovenia. Skutočnosť, že GDPR dáva členským štátom možnosť stanoviť výnimky vo vzťahu k orgánom verejnej moci a verejnoprávnym subjektom usadeným na ich území,[118] ako aj požiadavky týkajúce sa postupu, ktorý majú dozorné orgány dodržať pri ukladaní správnej pokuty,[119] vôbec neznamená, že by boli tieto štáty tiež oprávnené stanoviť takéto hmotnoprávne podmienky.

Pokiaľ ide o tieto podmienky, Súdny dvor poznamenal, že medzi skutočnosti vymenované v GDPR, ktoré má dozorný orgán zohľadniť pri ukladaní správnej pokuty prevádzkovateľovi, patrí „úmyselný alebo nedbanlivostný charakter porušenia“[120]. Naproti tomu nijaká z okolností neodkazuje na možnosť založiť zodpovednosť

[117] Porušenie uvedené v článku 83 ods. 4 až 6.
[118] Podľa článku 83 ods. 7 GDPR, ktorý stanovuje, že „každý členský štát môže stanoviť pravidlá, či a v akom rozsahu sa môžu správne pokuty uložiť orgánom verejnej moci a verejnoprávnym subjektom zriadeným [usadeným – *neoficiálny preklad*] v danom členskom štáte“.
[119] Podľa článku 83 ods. 8 GDPR v spojení s jeho odôvodnením 129.
[120] Článok 83 ods. 2 písm. b) GDPR.

prevádzkovateľa v prípade, že nedošlo z jeho strany k zavinenému konaniu. Iba porušenia ustanovení GDPR, ktorých sa dopustil prevádzkovateľ úmyselne alebo z nedbanlivosti, môžu viesť k uloženiu správnej pokuty tomuto prevádzkovateľovi podľa článku 83 tohto nariadenia.

Súdny dvor dodal, že tento výklad je podporený všeobecnou štruktúrou a účelom GDPR. V tejto súvislosti spresnil, že existencia systému sankcií podľa GDPR, ktorý umožňuje uložiť, ak to odôvodňujú osobitné okolnosti každého jednotlivého prípadu, správnu pokutu, podnecuje prevádzkovateľov a sprostredkovateľov k dodržiavaniu tohto nariadenia a že správne pokuty svojím odradzujúcim účinkom prispievajú k posilneniu ochrany dotknutých osôb. Normotvorca Únie však nepovažoval za potrebné stanoviť uloženie správnych pokút v prípade neexistencie zavinenia. Vzhľadom na skutočnosť, že GDPR sa usiluje o rovnocennú a zároveň jednotnú úroveň ochrany a na tento účel sa musí uplatňovať konzistentne v celej Únii, bolo by v rozpore s týmto účelom umožniť členským štátom stanoviť takýto režim ukladania pokút.

Okrem toho Súdny dvor rozhodol, že takúto pokutu možno uložiť prevádzkovateľovi v súvislosti so spracovateľskými operáciami s osobnými údajmi, ktoré v jeho mene vykonal sprostredkovateľ, okrem prípadov, v ktorých tento sprostredkovateľ v rámci týchto operácií vykonal spracúvanie na svoje vlastné účely alebo spracúval tieto údaje spôsobom nezlučiteľným s rámcom alebo spôsobmi spracúvania, ako boli určené prevádzkovateľom, alebo takým spôsobom, o ktorom sa nemožno rozumne domnievať, že by s ním tento prevádzkovateľ súhlasil. V tomto prípade sa sprostredkovateľ musí považovať za prevádzkovateľa takéhoto spracúvania.

Rozsudok z 5. decembra 2023 (veľká komora), Deutsche Wohnen (C-807/21, EU:C:2023:950)

Deutsche Wohnen SE (ďalej len „DW“) je realitná spoločnosť, ktorá prostredníctvom podielov v rôznych spoločnostiach vlastní nepriamo veľký počet komerčných priestorov a bytových jednotiek. V rámci svojej obchodnej činnosti spracúva osobné údaje nájomcov týchto komerčných priestorov a bytových jednotiek.

V nadväznosti na dve kontroly vykonané v rokoch 2017 a 2019 Berliner Beauftragte für den Datenschutz (dozorný orgán Berlín, Nemecko) konštatoval viaceré porušenia GDPR, ktorých sa dopustila DW. Rozhodnutím z 30. októbra 2019 jej tento dozorný orgán z tohto dôvodu uložil správne pokuty.

DW podala proti tomuto rozhodnutiu žalobu na Landgericht Berlin (Krajinský súd Berlín, Nemecko), ktorý vec odložil. Tento súd uviedol, že podľa nemeckého zákona[121] spáchanie správneho deliktu možno konštatovať len voči fyzickej osobe, a nie voči právnickej osobe. V prípade vzniku zodpovednosti právnickej osoby jej navyše možno pripísať len konanie členov jej orgánov alebo jej zástupcov. Staatsanwaltschaft Berlin

[121] Gesetz über Ordnungswidrigkeiten (zákon o správnych deliktoch) z 24. mája 1968 (BGBl. 1968 I, s. 481) v znení oznámenia z 19. februára 1987 (BGBl. 1987 I I, s. 602), a zákona z 19. júna 2020 (BGBl. 2020 I, s. 1350).

(Prokuratúra Berlín, Nemecko) podala proti tomuto rozhodnutiu odvolanie na Kammergericht Berlin (Vyšší krajinský súd Berlín, Nemecko). V tejto súvislosti sa tento súd obrátil na Súdny dvor s návrhom na začatie prejudiciálneho konania týkajúcim sa výkladu GDPR.

Súdny dvor zasadajúci vo veľkej komore vo svojom rozsudku rozhodol o podmienkach ukladania správnych pokút podľa GDPR. V prvom rade skúmal otázku, či členské štáty môžu podmieniť uloženie správnej pokuty právnickej osobe tým, aby bolo porušenie tohto nariadenia predtým pripísané identifikovanej fyzickej osobe. V druhom rade sa podobne ako v rozsudku Nacionalinis visuomenės sveikatos centras (pozri vyššie) zaoberá tiež otázkou, či sankcionované porušenie ustanovení GDPR musí byť spáchané úmyselne alebo z nedbanlivosti.

Pokiaľ ide o uloženie správnej pokuty právnickej osobe podľa GDPR, Súdny dvor najskôr uvádza, že zásady, zákazy a povinnosti stanovené v GDPR sú určené najmä „prevádzkovateľom“, ktorých zodpovednosť sa vzťahuje na každé spracúvanie osobných údajov, ktoré vykonávajú sami alebo ktoré sa uskutočňuje v ich mene. Práve na základe tejto zodpovednosti sa v prípade porušenia ustanovení GDPR ukladá prevádzkovateľovi podľa článku 83 tohto nariadenia správna pokuta. No na účely určenia takejto zodpovednosti normotvorca Únie nerozlišoval medzi fyzickými a právnickými osobami, pričom táto zodpovednosť je podmienená len tým, že tieto osoby samy alebo v spojení s inými osobami určia účely a prostriedky spracúvania osobných údajov.[122] Každá osoba, ktorá spĺňa túto podmienku, je teda v zásade zodpovedná okrem iného za akékoľvek porušenie GDPR, ktorého sa dopustila sama alebo ktoré bolo spáchané v jej mene. Na jednej strane to znamená, že právnické osoby sú zodpovedné nielen za porušenia, ktorých sa dopustili ich zástupcovia, riadiaci pracovníci alebo manažéri, ale aj akákoľvek iná osoba konajúca v rámci obchodnej činnosti týchto právnických osôb a na ich účet. Na druhej strane, pokiaľ možno právnické osoby kvalifikovať ako prevádzkovateľov, musí byť možné im v prípade takýchto porušení priamo uložiť správne pokuty podľa GDPR.

Následne Súdny dvor konštatoval, že žiadne ustanovenie GDPR neumožňuje vyvodiť záver, že uloženie správnej pokuty právnickej osobe ako prevádzkovateľovi je podmienené predchádzajúcim konštatovaním, že tohto porušenia sa dopustila identifikovaná fyzická osoba. Okrem toho normotvorca Únie neponechal členským štátom v tejto súvislosti priestor na voľnú úvahu. Skutočnosť, že GDPR dáva členským štátom možnosť stanoviť požiadavky týkajúce sa postupu, ktorý majú dozorné orgány uplatniť pri ukladaní správnej pokuty,[123] však vôbec neznamená, že by boli oprávnené stanoviť ďalšie hmotnoprávne podmienky okrem tých, ktoré sú stanovené v GDPR.

V tejto súvislosti Súdny dvor spresnil, že ak by sa členským štátom umožnilo, aby ako nevyhnutnú podmienku na uloženie správnej pokuty prevádzkovateľovi, ktorý je právnickou osobou, podľa článku 83 GDPR, jednostranne požadovali, aby sa predmetné

[122] Podľa článku 4 bodu 7 GDPR.
[123] Ako vyplýva z článku 58 ods. 4 a článku 83 ods. 8 GDPR v spojení s jeho odôvodnením 129.

porušenie predtým pripísalo alebo mohlo pripísať identifikovanej fyzickej osobe, bolo by to v rozpore s účelom GDPR. Okrem toho by takáto dodatočná požiadavka v konečnom dôsledku mohla oslabiť účinnosť a odradzujúci účinok správnych pokút uložených právnickým osobám ako prevádzkovateľom.

Napokon Súdny dvor zdôraznil, že pojem „podnik“ v zmysle článkov 101 a 102 ZFEÚ[124] nemá nijaký vplyv na otázku, či a za akých podmienok možno prevádzkovateľovi, ktorý je právnickou osobou, uložiť správnu pokutu podľa GDPR, a nie je relevantný na stanovenie výšky takejto pokuty.

Súdny dvor tak dospel k záveru, že GDPR[125] bráni vnútroštátnej právnej úprave, podľa ktorej možno právnickej osobe ako prevádzkovateľovi uložiť správnu pokutu za porušenie tohto nariadenia[126] len v prípade, že toto porušenie bolo predtým pripísané identifikovanej fyzickej osobe.

Pokiaľ ide o otázku, či členské štáty môžu stanoviť uloženie správnej pokuty aj v prípade, že sankcionované porušenie nebolo spáchané úmyselne alebo z nedbanlivosti, Súdny dvor v prvom rade pripomenul, že hmotnoprávne podmienky, ktoré dozorný orgán musí dodržiavať pri ukladaní takejto pokuty prevádzkovateľovi, sú upravené výlučne právom Únie a že členské štáty nemajú v tejto súvislosti nijaký priestor na voľnú úvahu. Súdny dvor na základe rovnakého odôvodnenia prijatého vo vyššie uvedenom rozsudku Nacionalinis visuomenės sveikatos centras konštatoval, že podľa článku 83 GDPR správnu pokutu možno uložiť len vtedy, ak sa preukáže, že prevádzkovateľ, ktorý je právnickou osobou a zároveň podnikom, sa úmyselne alebo z nedbanlivosti dopustil porušenia pravidiel obsiahnutých v tomto nariadení.

5. Skĺbenie právomocí vnútroštátnych dozorných orgánov s právomocami iných vnútroštátnych orgánov

Rozsudok zo 4. júla 2023 (veľká komora), Meta Platforms a i. (Všeobecné podmienky používania sociálnej siete) (C-252/21, EU:C:2023:537)

V tejto veci (pozri tiež rubriku V.5. s názvom „Spracúvanie osobných údajov na online sociálnych sieťach“) Súdny dvor pri rozhodovaní o právomoci orgánu na ochranu hospodárskej súťaže konštatovať nesúlad spracúvania osobných údajov s GDPR, zastával názor, že s výhradou dodržania povinnosti lojálnej spolupráce[127] s dozornými orgánmi pre ochranu údajov môže takýto orgán v rámci preskúmania, či došlo k zneužitiu

[124] Na ktorú sa odkazuje v odôvodnení 150 GDPR.
[125] Článok 58 ods. 2 písm. i) a článok 83 ods. 1 až 6 GDPR.
[126] Uvedené v článku 83 ods. 4 až 6 GDPR.
[127] Zakotvená v článku 4 ods. 3 ZEÚ.

dominantného postavenia podnikom[128], konštatovať, že všeobecné podmienky používania vypracované týmto podnikom v oblasti spracúvania osobných údajov a ich vykonávanie nie sú v súlade s týmto nariadením, ak je toto konštatovanie potrebné na preukázanie existencie takéhoto zneužitia. Ak však orgán na ochranu hospodárskej súťaže poukáže na porušenie GDPR v rámci konštatovania zneužitia dominantného postavenia, nenahrádza dozorné orgány.

Vzhľadom na zásadu lojálnej spolupráce platí, že ak orgány na ochranu hospodárskej súťaže majú pri výkone svojich právomocí preskúmať, či je správanie podniku v súlade s ustanoveniami GDPR, musia sa vzájomne dohodnúť a lojálne spolupracovať s dotknutými vnútroštátnymi dozornými orgánmi alebo vedúcim dozorným orgánom. Všetky tieto orgány sú tak povinné dodržiavať svoje príslušné právomoci a kompetencie tak, aby boli dodržané povinnosti vyplývajúce z GDPR, ako aj ciele tohto nariadenia, a aby bol zachovaný ich potrebný účinok. Z toho vyplýva, že ak sa vnútroštátny orgán na ochranu hospodárskej súťaže v rámci preskúmania, či určitý podnik zneužil dominantné postavenie, domnieva, že je potrebné preskúmať súlad správania tohto podniku s ustanoveniami GDPR, uvedený orgán musí overiť, či toto správanie alebo podobné správanie už boli predmetom rozhodnutia zo strany príslušného vnútroštátneho dozorného orgánu, vedúceho dozorného orgánu alebo Súdneho dvora. Ak je to tak, orgán na ochranu hospodárskej súťaže sa od neho nemôže odchýliť, avšak môže z nich vyvodiť vlastné závery z hľadiska uplatnenia práva hospodárskej súťaže.

Ak má vnútroštátny orgán na ochranu hospodárskej súťaže pochybnosti o rozsahu posúdenia vykonaného príslušným vnútroštátnym dozorným orgánom alebo vedúcim dozorným orgánom, pokiaľ je predmetné správanie alebo podobné správanie zároveň predmetom preskúmania zo strany týchto orgánov, alebo ak sa v prípade neexistencie vyšetrovania zo strany uvedených orgánov domnieva, že správanie podniku nie je v súlade s ustanoveniami GDPR, musí sa orgán na ochranu hospodárskej súťaže poradiť s týmito orgánmi a požiadať ich o spoluprácu, aby sa zbavil svojich pochybností alebo aby určil, či treba pred vykonaním vlastného posúdenia počkať na prijatie rozhodnutia zo strany dotknutého dozorného orgánu. Ak tieto dozorné orgány nevznesú námietku alebo neodpovedia v primeranej lehote, orgán na ochranu hospodárskej súťaže môže pokračovať vo vlastnom vyšetrovaní.

[128] V zmysle článku 102 ZFEÚ.

SÚDNY DVOR
EURÓPSKEJ ÚNIE

Riaditeľstvo výskumu a dokumentácie

Júl 2024