



Tematski prikaz

VARSTVO OSEBNIH PODATKOV

Pravica do varstva osebnih podatkov je temeljna pravica, katere spoštovanje je pomemben cilj Evropske unije.

Določena je z Listino Evropske unije o temeljnih pravicah (v nadaljevanju: Listina), katere člen 8 določa:

„1. Vsakdo ima pravico do varstva osebnih podatkov, ki se nanj nanašajo.

2. Osebnih podatki se morajo obdelovati pošteno, za določene namene in na podlagi privolitve prizadete osebe ali na drugi legitimni podlagi, določeni z zakonom. Vsakdo ima pravico dostopa do podatkov, zbranih o njem, in pravico zahtevati, da se ti podatki popravijo.

3. Spoštovanje teh pravil nadzira neodvisen organ.“

Ta temeljna pravica je tesno povezana s pravico do spoštovanja zasebnega življenja iz člena 7 Listine.

Pravica do varstva osebnih podatkov je določena tudi v členu 16(1) Pogodbe o delovanju Evropske unije (PDEU), ki je v zvezi s tem nadomestil člen 286 ES.

Kar zadeva sekundarno pravo, je Evropska skupnost sredi devetdesetih let sprejela razne instrumente za zagotavljanje varstva osebnih podatkov. Direktiva 95/46/ES o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov,¹ ki je bila sprejeta na podlagi člena 100a ES, je v tem pogledu osrednji pravni akt Unije na tem področju. Z njo so opredeljeni splošni pogoji, ki urejajo zakonitost obdelave teh podatkov in pravice zadevnih oseb ter določena ustanovitev neodvisnih nadzornih organov v državah članicah.

¹ Direktiva Evropskega parlamenta in Sveta 95/46/ES z dne 24. oktobra 1995 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov (UL, posebna izdaja v slovenščini, poglavje 13, zvezek 15, str. 355), prečiščena različica z dne 20. 11. 2003, razveljavljena s 25. majem 2018 (glej opombo 5).

Nato je Direktivo 95/46/ES dopolnila Direktiva 2002/58/ES,² s katero so bile harmonizirane določbe zakonodaje držav članic o varstvu pravice do zasebnosti, zlasti v zvezi z obdelavo osebnih podatkov na področju elektronskih komunikacij.³

Poleg tega je na področju območja svobode, varnosti in pravice (prejšnja člena 30 in 31 PEU) z Okvirnim sklepom 2008/977/PNZ⁴ (do maja 2018) urejeno varstvo osebnih podatkov na področju pravosodnega sodelovanja v kazenskih in policijskih zadevah.

Evropska unija je nedavno pripravila nov celovit pravni okvir na tem področju. Za to je leta 2016 sprejela Uredbo (EU) 2016/679⁵ o varstvu osebnih podatkov, s katero se razveljavlja Direktiva 95/46/ES in ki se bo neposredno uporabljala od 25. maja 2018, ter Direktivo (EU) 2016/680⁶ o varstvu podatkov v kazenskih zadevah, s katero je bil razveljaven Okvirni sklep 2008/977/PNZ in za katero je bil datum za prenos za države članice določen na 6. maj 2018.

Nazadnje, v okviru obdelave osebnih podatkov v institucijah in organih EU je varstvo osebnih podatkov zagotovljeno z Uredbo (ES) št. 45/2001.⁷ S to uredbo je bila zlasti omogočena ustanovitev Evropskega nadzornika za varstvo podatkov leta 2004. Januarja 2017 je Komisija predstavila predlog⁸ nove uredbe o razveljavitvi Uredbe št. 45/2001 in Sklepa št. 1247/2002/ES za posodobitev pravil na tem področju in njihovo uskladitev z novo ureditvijo, uvedeno z Uredbo (EU) 2016/679.

2 Direktiva 2002/58/ES Evropskega parlamenta in Sveta z dne 12. julija 2002 o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij (Direktiva o zasebnosti in elektronskih komunikacijah) (UL, posebna izdaja v slovenščini, poglavje 13, zvezek 29, str. 514), prečiščena različica z dne 19. 12. 2009.

3 Direktiva 2002/58/ES je bila spremenjena z Direktivo 2006/24/ES Evropskega parlamenta in Sveta z dne 15. marca 2006 o hrambi podatkov, pridobljenih ali obdelanih v zvezi z zagotavljanjem javno dostopnih elektronskih komunikacijskih storitev ali javnih komunikacijskih omrežij, in spremembi Direktive 2002/58/ES (UL L 105, 13.4.2006, str. 54). Sodišče je s sodbo z dne 8. aprila 2014, Digital Rights Ireland ter Seitlinger in drugi (C-293/12 in C-594/12, EU:C:2014:238), razglasilo, da ta direktiva ni veljavna, ker je resno posegala v pravico do zasebnega življenja in do varstva osebnih podatkov (glej razdelek I.1. tega tematskega prikaza, naslovljen „Skladnost sekundarnega prava Unije s pravico do varstva osebnih podatkov“).

4 Okvirni sklep Sveta 2008/977/PNZ z dne 27. novembra 2008 o varstvu osebnih podatkov, ki se obdelujejo v okviru policijskega in pravosodnega sodelovanja v kazenskih zadevah (UL L 350, 30.12.2008, str. 60), ki bo razveljaven 6. maja 2018 (glej opombo 6).

5 Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46 (UL L 119, 4.5.2016, str. 1), ki se uporablja od 25. maja 2018.

6 Direktiva (EU) 2016/680 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov, ki jih pristojni organi obdelujejo za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij, in o prostem pretoku takih podatkov ter o razveljavitvi Okvirnega sklepa Sveta 2008/977/PNZ (UL L 119, 4.5.2016, str. 89).

7 Uredba (ES) št. 45/2001 Evropskega parlamenta in Sveta z dne 18. decembra 2000 o varstvu posameznikov pri obdelavi osebnih podatkov v institucijah in organih Skupnosti in o prostem pretoku takih podatkov (UL, posebna izdaja v slovenščini, poglavje 13, zvezek 26, str. 102).

8 Predlog uredbe Evropskega parlamenta in Sveta o varstvu posameznikov pri obdelavi osebnih podatkov v institucijah, organih, uradih in agencijah Unije in o prostem pretoku takih podatkov ter o razveljavitvi Uredbe (ES) št. 45/2001 in Sklepa št. 1247/2002/ES (COM(2017) 8 final).

I. Pravica do varstva osebnih podatkov, priznana z Listino Evropske unije o temeljnih pravicah

1. Skladnost sekundarnega prava Unije s pravico do varstva osebnih podatkov

*Sodba z dne 9. novembra 2010 (veliki senat), Volker und Markus Schecke in Eifert (C-92/09 in C-93/09, EU:C:2010:662)*⁹

V tej zadevi sta spora o glavni stvari potekala med dvema kmetoma na eni strani in Land Hessen na drugi glede objave osebnih podatkov teh kmetov kot upravičencev do sredstev iz Evropskega kmetijskega jamstvenega sklada (EKJS) in Evropskega kmetijskega sklada za razvoj podeželja (EKSRP) na spletnem mestu Bundesanstalt für Landwirtschaft und Ernährung (zvezni urad za kmetijstvo in prehrano). Navedena kmeta sta nasprotovala tej objavi in zlasti zatrjevala, da ta ni utemeljena s prevladujočim javnim interesom. Land Hessen je menila, da objava navedenih podatkov izhaja iz uredb (ES) št. 1290/2005¹⁰ in 259/2008¹¹, s katerima je urejeno financiranje skupne kmetijske politike in naložena objava informacij o fizičnih osebah, ki so upravičene do sredstev iz EKJS in EKSRP.

V teh okoliščinah je Verwaltungsgericht Wiesbaden (upravno sodišče v Wiesbadnu, Nemčija) Sodišču predložilo več vprašanj v zvezi z veljavnostjo nekaterih določb Uredbe (ES) št. 1290/2005 in Uredbe (ES) št. 259/2008, s katerimi se nalaga objava tovrstnih informacij, med drugim na spletnih mestih nacionalnih organov.

Sodišče je v zvezi z usklajevanjem med pravico do varstva osebnih podatkov, ki je priznana z Listino, in obveznostjo preglednosti na področju evropskih sredstev ugotovilo, da objava poimenskih podatkov o upravičencih do sredstev iz skladov in o zneskih, ki so jih ti prejeli, glede na to, da je spletno mesto prosto dostopno tretjim osebam, pomeni poseg v pravico zadevnih upravičencev do zasebnega življenja na splošno in, natančneje, pravico do varstva osebnih podatkov (točke od 56 do 64).

Da bi bil tak poseg upravičen, mora biti predpisan z zakonom, spoštovati mora bistveno vsebino navedenih pravic ter biti – ob upoštevanju načela sorazmernosti – potreben in dejansko ustrezati ciljem splošnega interesa, ki jih priznava Unija, pri čemer morajo biti odstopanja in omejitve teh pravic strogo omejeni na tisto, kar je nujno potrebno (točka 65). Sodišče je v tem okviru menilo, da imajo davkoplačevalci v demokratični družbi sicer pravico biti obveščeni o uporabi javnih sredstev, vendar bi morala Svet in Komisija uravnotežiti različne zadevne interese, kar pomeni, da bi morala pred sprejetjem spornih določb preveriti, ali to, da država članica objavi te podatke na eni sami spletni strani, ne presega tistega, kar je potrebno za uresničitev legitimnih ciljev, ki se jim sledi (točke 77, 79, 85 in 86).

Tako je Sodišče ugotovilo, da so nekatere določbe Uredbe (ES) št. 1290/2005 in Uredbe (ES) št. 259/2008 v celoti neveljavne, ker te določbe v zvezi s fizičnimi osebami, ki so upravičene do sredstev iz EKJS in EKSRP, določajo obveznost objave osebnih podatkov vseh upravičencev, ne da bi se opravilo razlikovanje glede na ustrezna merila, kot so obdobja, v katerih so prejeli sredstva, pogostost ali vrsta in višina sredstev (točka 92 in točka 1 izreka). Vendar je Sodišče odločilo, da ni mogoče izpodbijati učinkov objave

⁹ Ta sodba je bila predstavljena v Letnem poročilu 2010, str. 11.

¹⁰ Uredba Sveta (ES) št. 1290/2005 z dne 21. junija 2005 o financiranju skupne kmetijske politike (UL L 209, 11.8.2005, str. 1), ki je bila razveljavljena z Uredbo (EU) št. 1306/2013 Evropskega parlamenta in Sveta z dne 17. decembra 2013 o financiranju, upravljanju in spremljanju skupne kmetijske politike (UL L 347, 20.12.2013, str. 549).

¹¹ Uredba Komisije (ES) št. 259/2008 z dne 18. marca 2008 o podrobnih pravilih za uporabo Uredbe Sveta (ES) št. 1290/2005 glede objavljanja informacij o upravičencih do sredstev iz Evropskega kmetijskega jamstvenega sklada (EKJS) in Evropskega kmetijskega sklada za razvoj podeželja (EKSRP) (UL L 76, 19.3.2008, str. 28), razveljavljena z Izvedbeno uredbo Komisije (EU) št. 908/2014 z dne 6. avgusta 2014 o pravilih za uporabo Uredbe (EU) št. 1306/2013 Evropskega parlamenta in Sveta v zvezi s plačilnimi agencijami in drugimi organi, finančnim upravljanjem, potrjevanjem obračunov, pravili o kontrolah, varščinami in preglednostjo (UL L 255, 28.8.2014, str. 59).

seznamov upravičencev do teh sredstev, ki so jo nacionalni organi opravili na podlagi teh določb pred izrekom sodbe (točka 94 in točka 2 izreka).

Sodba z dne 17. oktobra 2013, Schwarz (C-291/12, EU:C:2013:670)

M. Schwarz je pri mestu Bochum (Nemčija) zaprosil za izdajo potnega lista, vendar je odklonil odvzem prstnih odtisov. Ker je mesto njegovo prošnjo zavrnilo, je M. Schwarz pri Verwaltungsgericht Gelsenkirchen (upravno sodišče v Gelsenkirchnu, Nemčija) vložil tožbo, da bi se tej občini naložilo, naj mu potni list izda brez odvzema prstnih odtisov. M. Schwarz je pri tem sodišču izpodbijal veljavnost Uredbe (ES) št. 2252/2004,¹² s katero je bila uvedena obveznost odvzema prstnih odtisov prosilcem za izdajo potnih listov, in med drugim trdil, da se s to uredbo kršita pravica do varstva osebnih podatkov in pravica do spoštovanja zasebnega življenja.

V teh okoliščinah je Verwaltungsgericht Gelsenkirchen pri Sodišču vložilo predlog za sprejetje predhodne odločbe, da bi izvedelo, ali je navedena uredba v delu, v katerem se z njo prosilca za izdajo potnih listov zavezuje, da da svoje prstne odtise in določa njihovo shranjevanje v potnem listu, veljavna, zlasti z vidika Listine.

Sodišče je temu pritrdilo in razsodilo, da to, da nacionalni organi odvzamejo in shranijo prstne odtise, kakor je določeno v členu 1(2) Uredbe (ES) št. 2252/2004, sicer pomeni poseg v pravici do spoštovanja zasebnega življenja in varstva osebnih podatkov, vendar je ta poseg upravičen s ciljem zaščite potnih listov pred zlorabo.

Najprej, taka omejitev, predpisana z zakonom, sledi cilju splošnega interesa, ki ga priznava Unija, saj se z njo preprečuje zlasti nezakonit vstop oseb na ozemlje Unije (točke od 35 do 38). Dalje, odvzem in shranjevanje prstnih odtisov sta primerna za doseganje tega cilja. Po eni strani namreč metoda preverjanja identitete s prstnimi odtisi, čeprav ni popolnoma zanesljiva, znatno zmanjšuje tveganje sprejetja nepooblaščenih oseb. Po drugi strani neujemanje prstnih odtisov imetnika potnega lista s podatki, vključenimi v ta dokument, ne pomeni, da se zadevni osebi samodejno zavrne vstop na ozemlje Unije, temveč bo posledica samo ta, da temu sledi poglobljena kontrola, namenjena dokončni ugotovitvi identitete navedene osebe (točke od 42 do 45).

Nazadnje, kar zadeva potrebnost take obdelave, Sodišče ni bilo seznanjeno z obstojem ukrepov, ki bi bili dovolj učinkoviti in ki bi obenem pomenili manjši poseg v pravici, priznani s členoma 7 in 8 Listine, kot ukrepi, ki izhajajo iz metode, ki temelji na prstnih odtisih (točka 53). Člen 1(2) Uredbe (ES) št. 2252/2004 ne zajema obdelav odvzetih prstnih odtisov, ki bi presegle tisto, kar je potrebno za uresničitev zasledovanega cilja. V navedeni uredbi je namreč izrecno določeno, da se lahko prstni odtisi uporabijo samo za preverjanje verodostojnosti potnega lista in identitete njegovega imetnika. Poleg tega člen 1(2) Uredbe zagotavlja varstvo pred nevarnostjo, da bi podatke, ki vsebujejo prstne odtise, brale nepooblaščen osebe, in določa, da se zadevni podatki hranijo samo v potnem listu, ki ostaja v izključni posesti imetnika (točke od 54 do 57, 60 in 63).

¹² Uredba Sveta (ES) št. 2252/2004 z dne 13. decembra 2004 o standardih za varnostne značilnosti in biometrične podatke v potnih listih in potovalnih dokumentih, ki jih izdajo države članice (UL L 385, 29.12.2004, str. 1), kakor je bila spremenjena z Uredbo (ES) št. 444/2009 Evropskega parlamenta in Sveta z dne 6. maja 2009 (UL L 142, 6.6.2009, str. 1).

Sodba z dne 8. aprila 2014 (veliki senat), Digital Rights Ireland in Seitlinger in drugi (združeni zadevi C-293/12 in C-594/12, EU:C:2014:238)¹³

Ta sodba se navezuje na predloga za presojo veljavnosti Direktive 2006/24/ES o hrambi podatkov glede na temeljni pravici spoštovanja zasebnega življenja in varstva osebnih podatkov, ki sta bila podana v okviru nacionalnih sporov pred irskim in avstrijskim sodiščem. V zadevi C-392/12 je bil High Court (višje sodišče, Irska) predložen spor med družbo Digital Rights in irskimi organi glede zakonitosti ukrepov v zvezi s hrambo podatkov o elektronskih komunikacijah. V zadevi C-594/12 je bilo pri Verfassungsgerichtshof (ustavno sodišče, Avstrija) vloženi več pravnih sredstev na ustavni ravni, s katerimi je bila predlagana razglasitev ničnosti nacionalnega predpisa, s katerim je bila Direktiva 2006/24/ES prenesena v avstrijsko pravo.

Irsko in avstrijsko sodišče sta s svojima predlogoma za sprejetje predhodne odločbe Sodišče vprašala o veljavnosti Direktive 2006/24/ES z vidika členov 7, 8 in 11 Listine. Natančneje, navedeni sodišči sta Sodišče vprašali, ali obveznost, ki je s to direktivo naložena ponudnikom javno dostopnih elektronskih komunikacijskih storitev ali javnih komunikacijskih omrežij, da v določenem obdobju hranijo podatke o zasebnem življenju osebe in njenih komunikacijah ter da omogočijo dostop do njih pristojnim nacionalnim organom, pomeni neutemeljeno poseganje v navedeni temeljni pravici. Zadevni podatki so med drugim podatki, potrebni za sledenje ter prepoznanje vira in cilja komunikacije, za ugotovitev datuma, časa, trajanja in vrste komunikacije, za razpoznavo komunikacijske opreme uporabnikov ter za ugotovitev lokacije opreme za mobilno komunikacijo, med katerimi so predvsem ime in naslov naročnika ali registriranega uporabnika, kličoča in klicana telefonska številka ter naslov IP za internetne storitve. Na podlagi teh podatkov je mogoče zlasti ugotoviti, s katero osebo je komuniciral naročnik ali registrirani uporabnik in katero sredstvo je uporabil za to, ter ugotoviti trajanje komunikacije in kraj, s katerega je potekala komunikacija. Poleg tega je s temi podatki mogoče ugotoviti pogostost komunikacij naročnika ali registriranega uporabnika z določenimi osebami v danem obdobju.

Sodišče je najprej razsodilo, da pomenijo določbe Direktive 2006/24/ES zaradi nalaganja takih obveznosti ponudnikom posebej resno poseganje v temeljni pravici spoštovanja zasebnega življenja in varstva osebnih podatkov, zagotovljeni s členoma 7 in 8 Listine. Sodišče je v tem okviru sicer ugotovilo, da bi bilo to poseganje mogoče upravičiti z uresničevanjem cilja v splošnem interesu, kot je boj proti organiziranemu kriminalu. Sodišče je v zvezi s tem navedlo, prvič, da hranjenje podatkov, ki je naloženo z Direktivo, ne more posegati v bistveno vsebino temeljnih pravic spoštovanja zasebnega življenja in varstva osebnih podatkov, ker Direktiva ne dovoljuje seznanjanja z vsebino elektronskih komunikacij in določa, da morajo ponudniki storitev ali omrežij spoštovati nekatera načela varovanja in varnosti podatkov. Drugič, Sodišče je opozorilo, da hranjenje podatkov za njihov morebitni prenos pristojnim nacionalnim organom dejansko ustreza cilju v splošnem interesu, in sicer boju proti hudemu kriminalu, in tako nazadnje javni varnosti (točke od 38 do 44).

Sodišče je kljub temu odločilo, da je zakonodajalec Unije s sprejetjem Direktive o hrambi podatkov presegel meje, ki jih določa spoštovanje načela sorazmernosti. Zato je Sodišče ugotovilo, da Direktiva ni veljavna in štelo, da občutno in posebej resno poseganje v temeljne pravice, ki ga povzroča, ni dovolj natančno določeno v predpisih, da bi bilo zagotovljeno, da je poseganje dejansko omejeno na to, kar je nujno potrebno (točka 65). Direktiva 2006/24/ES je namreč na splošno zajemala vse osebe in vsa sredstva elektronske komunikacije ter vse podatke o prometu brez razlikovanja, omejitve ali izjeme v zvezi s ciljem boja proti hudim kaznivim dejanjem (točke od 57 do 59). Poleg tega ni bilo z Direktivo določeno nobeno objektivno merilo, s katerim bi se zagotavljalo, da bi imeli pristojni državni organi dostop do podatkov in bi jih lahko uporabili samo zaradi preprečevanja, odkrivanja ali pregona kršitev, ki jih je mogoče šteti za dovolj hude, da upravičujejo tako poseganje, ne vsebinski in postopkovni pogoji za tak dostop ali uporabo (točke od 60 do 62). Nazadnje, Direktiva je glede trajanja hrambe podatkov določala,

¹³ Ta sodba je bila predstavljena v Letnem poročilu 2014, str. 55.

da se ti hranijo najmanj šest mesecev, ne da bi se kakor koli razlikovalo med kategorijami podatkov glede na osebe, ki jih zadevajo, ali na možno uporabnost podatkov za zastavljeni cilj (točki 63 in 64).

Poleg tega je Sodišče v zvezi z zahtevami, ki izhajajo iz člena 8(3) Listine, ugotovilo, da Direktiva 2006/24/ES ni določala zadostnih jamstev, ki bi omogočala zagotovitev učinkovitega varovanja podatkov pred tveganji zlorabe ter vsakršnim nezakonitim dostopom do teh podatkov in njihovo nezakonito uporabo, niti ni nalagala, da se podatki hranijo na ozemlju Unije.

Zato navedena direktiva ni v celoti zagotavljala nadzora nad spoštovanjem zahtev glede varovanja in varnosti od neodvisnega organa, kar pa se izrecno zahteva z Listino (točke od 66 do 68).

2. Pravica do varstva osebnih podatkov pri izvajanju prava Unije

Sodba z dne 21. decembra 2016 (veliki senat), Tele2 Sverige (združeni zadevi C-203/15 in C-698/15, EU:C:2016:970)¹⁴

Sodišču sta bili po sodbi Digital Rights Ireland in Seitlinger in drugi, s katero je bila ugotovljena neveljavnost Direktive 2006/24/ES (glej zgoraj), predloženi zadevi v zvezi s splošno obveznostjo, naloženo ponudnikom elektronskih komunikacijskih storitev na Švedskem in v Združenem kraljestvu, da hranijo podatke v zvezi s temi komunikacijami, katerih hramba je bila določena z neveljavno direktivo.

Dan po razglasitvi sodbe Digital Rights Ireland in Seitlinger in drugi je telekomunikacijsko podjetje Tele2 Sverige švedskemu organu za nadzor pošte in telekomunikacij sporočilo svojo odločitev, da ne bo več hranilo podatkov, in namero, da izbriše vse že registrirane podatke (zadeva C-203/15). Švedsko pravo je namreč ponudnikom telekomunikacijskih storitev nalagalo, da sistematično in kontinuirano ter brez vsakršne izjeme hranijo vse podatke o prometu in podatke o lokaciji vseh naročnikov in registriranih uporabnikov glede vseh elektronskih komunikacijskih sredstev. V zadevi C-698/15 so tri osebe vložile tožbo zoper britanski sistem hranjena podatkov, s katerim je bil minister za notranje zadeve pooblaščen, da javnim telekomunikacijskim operaterjem naloži hranjenje vseh podatkov v zvezi s komunikacijami največ dvanajst mesecev, medtem ko je bila hramba vsebine teh komunikacij izključena.

Sodišče je na predlog Kammarrätten i Stockholm (višje upravno sodišče v Stockholmu, Švedska) in Court of Appeal (England and Wales) (Civil Division) (civilni oddelek višjega sodišča za Anglijo in Wales, združeno kraljestvo) odločalo o razlagi člena 15(1) Direktive 2002/58/ES, tako imenovane direktive o zasebnosti in elektronskih komunikacijah, s katero je državam članicam omogočeno, da določijo nekatere izjeme od obveznosti iz te direktive, v skladu s katero je treba zagotoviti zaupnost elektronskih komunikacij in z njimi povezanih podatkov o prometu.

Sodišče je v sodbi najprej razsodilo, da člen 15(1) Direktive 2002/58/ES ob upoštevanju členov 7, 8 in 11 ter člena 52(1) Listine nasprotuje nacionalni ureditvi, kakršna je švedska, ki z namenom boja proti kriminalu določa splošno in neselektivno hrambo vseh podatkov o prometu in podatkov o lokaciji vseh naročnikov in registriranih uporabnikov glede vseh elektronskih komunikacijskih sredstev. Po mnenju Sodišča taka nacionalna ureditev presega meje nujno potrebnega in je torej ni mogoče šteti za upravičeno v demokratični družbi, kot to zahteva navedeni člen 15(1) ob upoštevanju zgoraj navedenih členov Listine (točke od 99 do 105, 107 in 112 ter točka 1 izreka).

Navedena določba glede na iste člene Listine nasprotuje tudi nacionalni zakonodaji, ki ureja varstvo in varnost podatkov o prometu in podatkov o lokaciji, ter zlasti dostop pristojnih nacionalnih organov do

¹⁴ Ta sodba je bila predstavljena v Letnem poročilu 2016, str. 55.

hranjenih podatkov, pri tem pa v okviru boja proti kriminalu navedenega dostopa ne pogojuje z nameni boja proti hudemu kriminalu, ne določa, da mora nadzor nad navedenim dostopom predhodno opraviti sodišče ali neodvisni upravni organ, in ne zahteva, da se zadevni podatki hranijo na ozemlju Unije (točke od 118 do 122 in 125 ter točka 2 izreka).

Vendar je Sodišče razsodilo, da člen 15(1) Direktive 2002/58/ES ne nasprotuje ureditvi, ki dopušča preventivno ciljno hrambo podatkov o prometu in podatkov o lokaciji za boj proti hudemu kriminalu, če se hramba podatkov glede kategorij hranjenih podatkov, uporabljenih navedenih komunikacijskih sredstev, vpletenih oseb in trajanja zadevne hrambe omeji le na to, kar je nujno potrebno. Za izpolnjevanje teh zahtev mora ta nacionalna ureditev, prvič, določati jasna in natančna pravila, ki omogočajo učinkovito varstvo podatkov pred tveganji zlorabe. Zlasti mora biti določeno, v katerih okoliščinah in pod katerimi pogoji se lahko preventivno sprejme ukrep hrambe podatkov in s tem zagotovi, da se ta ukrep omeji na nujno potrebno. Drugič, glede vsebinskih pogojev, ki jih mora izpolnjevati nacionalna ureditev, da zagotovi, da je omejena na nujno potrebno, mora hramba podatkov vedno ustrezati objektivnim merilom, ki določajo razmerje med podatki, ki jih je treba hraniti, in uresničevanim ciljem. Zlasti morajo taki pogoji v praksi dejansko omejiti obseg ukrepa in s tem zadevno javnost. Glede te omejitve mora nacionalna zakonodaja temeljiti na objektivnih elementih, na katerih podlagi se lahko cilja javnost, katere podatki lahko izkažejo zvezo, vsaj posredno, s hudimi kaznivimi dejanji, tako ali drugače prispevajo k boju proti hudemu kriminalu ali preprečijo resno nevarnost za javno varnost (točke od 108 do 111).

II. Obdelava osebnih podatkov v smislu Direktive št. 95/46/ES

1. Obdelava osebnih podatkov, ki so izključeni s področja uporabe Direktive št. 95/46/ES

Sodba z dne 30. maja 2006 (veliki senat), Parlament/Svet (C-317/04 in C-318/04, EU:C:2006:346)

Združene države so po terorističnih napadih 11. septembra 2001 sprejele zakonodajo, ki določa, da morajo letalski prevozniki, ki zagotavljajo povezave v Združene države ali iz njih oziroma prečkajo njihovo ozemlje, ameriškim organom zagotoviti elektronski dostop do podatkov svojih rezervacijskih sistemov in sistemov za nadzor odhodov, imenovanih „Passenger Name Records“ (PNR).

Ker je Komisija menila, da bi te določbe lahko privedle do kolizije z evropsko zakonodajo in zakonodajo držav članic s področja varstva podatkov, je začela pogajanja z ameriški organi. Komisija je ob koncu teh pogajanj 14. maja 2004 sprejela Odločbo 2004/535/ES,¹⁵ s katero je ugotovila, da urad za carinsko in mejno zaščito Združenih držav Amerike (United States Bureau of Customs and Border Protection, v nadaljevanju: CBP) zagotavlja ustrezno raven varstva za podatke PNR, prenesene iz Skupnosti (v nadaljevanju: odločba o ustreznosti). Dalje, Svet je 17. maja 2004 sprejel Sklep 2004/496/ES¹⁶ o sklenitvi Sporazuma med Evropsko skupnostjo in Združenimi državami o obdelavi in prenosu podatkov PNR s strani letalskih prevoznikov s sedežem na ozemlju držav članic Uradu CBP.

¹⁵ Odločba Komisije 2004/535/ES z dne 14. maja 2004 o ustreznem varstvu osebnih podatkov, vsebovanih v evidenci imen letalskih potnikov, posredovani uradu za carinsko in mejno zaščito Združenih držav Amerike (UL L 235, 6.7.2004, str. 11).

¹⁶ Sklep Sveta 2004/496/ES z dne 17. maja 2004 o sklenitvi Sporazuma med Evropsko skupnostjo in Združenimi državami Amerike o obdelavi in prenosu podatkov PNR s strani letalskih prevoznikov Uradu za carine in varovanje meja pri Ministrstvu Združenih držav za domovinsko varnost (UL L 183, 20.5.2004, str. 83).

Evropski parlament je Sodišču predlagal, naj zgoraj navedeno odločbo in sklep razglasi za nična in pri tem med drugim zatrjeval, da je bila odločba o ustreznosti sprejeta *ultra vires*, da člen 95 ES (postal člen 114 PDEU) ni ustrezna pravna podlaga za sklep o sklenitvi sporazuma in da je vsekakor podana kršitev temeljnih pravic.

Kar zadeva odločbo o ustreznosti, je Sodišče najprej preverilo, ali je Komisija lahko veljavno sprejela odločbo na podlagi Direktive 95/46/ES. V tem okviru je ugotovilo, da iz odločbe o ustreznosti izhaja, da predstavlja prenos podatkov PNR Uradu CBP obdelavo, katere predmet so javna varnost in dejavnosti države na področju kazenskega prava. Sodišče je menilo, da tudi če so podatke PNR najprej zbirale letalske družbe v okviru dejavnosti, ki sodi v pravo Unije, in sicer prodaje letalskih vozovnic, ki dajejo pravico do storitev, je imela obdelava podatkov, ki se je upoštevala v odločbi o ustreznosti, povsem drugo naravo. Ta odločba se namreč ni nanašala na obdelavo podatkov, potrebno za opravljanje storitev, ampak na obdelavo podatkov, ki se šteje za nujno za zaščito javne varnosti in za namene kazenskega pregona (točki 56 in 57).

Sodišče je v zvezi s tem ugotovilo, da to, da so podatke PNR zbrali zasebni subjekti za ekonomske namene in da so jih ti prenesli v tretjo državo, ni nasprotovalo temu, da se zadevni prenos šteje za obdelavo podatkov, ki je izključena s področja uporabe te direktive. Ta prenos je namreč spadal v okvir, ki so ga določili javni organi in ki se je nanašal na javno varnost. Zato je Sodišče odločilo, da odločba o ustreznosti ne spada na področje uporabe Direktive, ker je šlo za obdelavo osebnih podatkov, ki je izključena s področja uporabe Direktive. Sodišče je zato odločbo o ustreznosti razglasilo za nično (točki 58 in 59).

Sodišče je v zvezi s Sklepom Sveta ugotovilo, da člen 95 ES v povezavi s členom 25 Direktive 95/46/ES ne more biti podlaga za pristojnost Skupnosti za sklenitev zadevnega sporazuma z Združenimi državami. Ta sporazum se je namreč nanašal na isti prenos podatkov kot odločba o ustreznosti in torej obdelave podatkov, ki so bile izključene s področja uporabe Direktive. Zato je Sodišče Sklep Sveta o sklenitvi sporazuma razglasilo za ničn (točke od 67 do 69).

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

F. Ryneš je zaradi vrste napadov na svojo hišo namestil nadzorno kamero. Po novem napadu na njegovo hišo je bilo mogoče s posnetki navedene kamere identificirati dva osumljenca, zoper katera je bil sprožen kazenski postopek. Eden od osumljencev je izpodbijal zakonitost obdelave podatkov, posnetih z nadzorno kamero, pri češkem uradu za varstvo osebnih podatkov, ki je ugotovil, da je F. Ryneš kršil pravila o varstvu osebnih podatkov in mu naložil globo.

Nejvyšší správní soud (vrhovno upravno sodišče, Češka republika), ki mu je bila predložena pritožba F. Ryneša zoper odločbo Městský soud v Praze (občinsko sodišče v Pragi, Češka republika), s katero je bila potrjena odločba urada, je Sodišču predložilo vprašanje, ali snemanje, ki ga je F. Ryneš izvajal zaradi varovanja svojega življenja, zdravja in premoženja, pomeni obdelavo, ki ni zajeta z Direktivo 95/46/ES, ker gre za snemanje, ki ga je izvajala fizična oseba pri opravljanju dejavnosti, ki so izključno osebne ali domače v smislu člena 3(2), druga alineja, navedene direktive.

Sodišče je razsodilo, da uporaba videonadzornega sistema – ki vodi do slikovnega snemanja oseb, ki se s krožnim snemanjem shranjuje na snemalno napravo, kot je trdi disk, in ki ga fizična oseba namesti na družinsko hišo zaradi varovanja premoženja, zdravja in življenja lastnikov hiše – s katerim se nadzira tudi javni prostor, ne pomeni obdelave podatkov, ki se opravi med potekom popolnoma osebne ali domače dejavnosti (točka 35 in izrek).

V zvezi s tem je Sodišče opozorilo, da varstvo temeljne pravice do zasebnega življenja, zagotovljene s členom 7 Listine, zahteva, da se izjeme od varstva osebnih podatkov in njegove omejitve določijo v mejah

tega, kar je nujno potrebno. Ker je treba določbe Direktive 95/46/ES, ki urejajo obdelavo osebnih podatkov, ki lahko pomeni poseg v temeljne svoboščine, zlasti pravico do zasebnosti, nujno razlagati ob upoštevanju temeljnih pravic, ki so vključene v navedeno listino, je treba izjemno, določeno v členu 3(2), druga alineja, te direktive, razlagati restriktivno. Poleg tega je že v besedilu te določbe iz uporabe Direktive 95/46 izvzeta obdelava podatkov, opravljena med potekom „popolnoma“ osebne ali domače dejavnosti. Če videonadzorni sistem zajema, čeprav delno, javni prostor in je tako usmerjen iz zasebnega okolja tistega, ki tako opravi obdelavo podatkov, ga ni mogoče šteti za popolnoma „osebno ali domačo“ dejavnost v smislu navedene določbe (točke 30, 31 in 33).

2. Pojem „osebni podatki“

Sodba z dne 19. oktobra 2016, Breyer (C-582/14, EU:C:2016:779)¹⁷

P. Breyer je pri nemških civilnih sodiščih vložil tožbo, s katero je predlagal, naj se Zvezni republiki Nemčiji prepove, da hrani računalniške podatke, ki so bili posredovani po vsakem dostopu do spletnih mest nemških zveznih organov, oziroma da za hrambo teh podatkov zadolži tretje osebe. Ponudnik storitev spletnih medijev nemških zveznih služb je namreč zaradi odvratanja napadov in omogočanja kazenskega pregona napadalcev beležil podatke, ki jih tvorijo „dinamični“ IP-naslov – to je naslov, ki se spreminja ob vsaki naslednji povezavi – ter datum in ura dostopa do spletnega mesta. Drugače kakor statični IP-naslovi dinamični IP-naslovi načeloma ne omogočajo povezave prek datotek, dostopnih javnosti, med danim računalnikom in fizičnim priključkom na omrežje, ki ga uporablja ponudnik dostopa do interneta. Zabeleženi podatki ponudniku spletnih medijev niso dajali možnosti identifikacije uporabnika. Vendar je imel ponudnik dostopa do interneta na voljo dodatne informacije, ki so skupaj s tem IP-naslovom omogočale identifikacijo navedenega uporabnika.

V teh okoliščinah je Bundesgerichtshof (zvezno vrhovno sodišče, Nemčija), ki je odločalo o reviziji, Sodišču predložilo vprašanje, ali IP-naslov, ki ga je ponudnik storitev spletnih medijev shranil ob dostopu neke osebe do njegovega spletnega mesta, zanj pomeni osebni podatek.

Sodišče je najprej navedlo, da za to, da bi bilo mogoče neki podatek šteti za „osebni podatek“ v smislu člena 2(a) Direktive 95/46/ES, ni nujno, da se vse informacije, ki omogočajo identifikacijo posameznika, na katerega se nanašajo osebni podatki, znajdejo v rokah samo ene osebe. To, da dodatnih informacij, potrebnih za identifikacijo uporabnika spletnega mesta, nima ponudnik storitev spletnih medijev, ampak ponudnik dostopa do interneta tega uporabnika, tako ne izključuje, da dinamični IP-naslovi, ki jih zabeleži ponudnik storitev spletnih medijev, zanj pomenijo osebne podatke v smislu člena 2(a) Direktive 95/46/ES (točki 43 in 44).

Sodišče je zato ugotovilo, da dinamični IP-naslov, ki ga je ponudnik storitev spletnih medijev zabeležil ob dostopu neke osebe do spletnega mesta, ki ga ta ponudnik daje na voljo javnosti, glede tega ponudnika pomeni osebni podatek v smislu člena 2(a) Direktive 95/46/ES, če ima na voljo pravna sredstva, ki mu omogočajo identifikacijo posameznika, na katerega se nanašajo osebni podatki, z dodatnimi informacijami, ki jih ima na voljo ponudnik dostopa do interneta tega posameznika (točka 49 in točka 1 izreka).

¹⁷ Ta sodba je bila predstavljena v Letnem poročilu 2016, str. 54.

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

P. Nowak, pripravnik za poklic računovodje, ni opravil izpita, ki ga je organizirala irska zbornica računovodij, finančnikov in revizorjev. Na podlagi člena 4 zakona o varstvu podatkov je vložil zahtevo za dostop do vseh osebnih podatkov, ki se nanj nanašajo in ki jih ima zbornica računovodij, finančnikov in revizorjev. Ta zbornica je P. Nowaku posredovala nekatere dokumente, zavrnila pa je posredovanje njegovega izpitnega izdelka z obrazložitvijo, da ta ne vsebuje osebnih podatkov v smislu zakona o varstvu podatkov.

Ker je tudi pooblaščenec za varstvo podatkov njegovo zahtevo zavrnil iz istih razlogov, se je P. Nowak obrnil na nacionalna sodišča. Supreme Court (vrhovno sodišče, Irska), ki je odločalo o pritožbi P. Nowaka, je Sodišču predložilo vprašanje, ali je treba člen 2(a) Direktive 95/46/ES razlagati tako, da so v okoliščinah, kakršne so obravnavane v postopku v glavni stvari, pisni odgovori, ki jih je na poklicnem izpitu dal kandidat, ter morebitni komentarji popravljavca, ki so s temi odgovori povezani, osebni podatki v smislu te določbe.

Sodišče je navedlo, , prvič, da za to, da bi bilo mogoče neki podatek šteti za „osebni podatek“ v smislu člena 2(a) Direktive 95/46/ES, ni nujno, da se vse informacije, ki omogočajo identifikacijo zadevne osebe, znajdejo v rokah samo ene osebe. Poleg tega ni sporno, da tudi če popravljavec ob ocenjevanju odgovorov, ki jih je kandidat dal v okviru izpita, ne pozna njegove identitete, pa subjekt, ki organizira izpit, v tem primeru zbornica računovodij, finančnikov in revizorjev, ima potrebne informacije, na katerih podlagi lahko brez težav in dvomov identificira tega kandidata zaradi njegove identifikacijske številke, ki je na izpitnem izdelku ali naslovni strani tega izdelka, in mu tako pripiše njegove odgovore.

Drugič, Sodišče je ugotovilo, da so pisni odgovori, ki jih je na poklicnem izpitu dal kandidat, informacije, ki so povezane z njim. Vsebina teh odgovorov namreč odraža stopnjo znanja in sposobnosti kandidata na danem področju ter, odvisno od primera, njegov proces razmišljanja, presojo in sposobnost kritičnega mišljenja. Dalje, namen zbiranja navedenih odgovorov je oceniti strokovne sposobnosti kandidata in njegovo zmožnost opravljanja zadevnega poklica. Poleg tega uporaba teh informacij, s katero se zlasti ugotovi uspeh ali neuspeh kandidata na zadevnem izpitu, lahko vpliva na pravice in interese tega kandidata, saj je zaradi nje mogoče določiti ali vplivati na primer na možnosti dostopa do želenega poklica oziroma zaposlitve. Ugotovitev, da so pisni odgovori, ki jih je na poklicnem izpitu dal kandidat, informacije, ki se nanj nanašajo zaradi svoje vsebine, namena in posledic, velja, tudi kadar gre za izpit z dostopnimi viri.

Tretjič, v zvezi s komentarji popravljavca glede odgovorov kandidata je Sodišče ugotovilo, da so ti tako kot odgovori, ki jih na izpitu da kandidat, informacije, ki se nanašajo na tega kandidata, saj odražajo mnenje ali presojo popravljavca o individualni uspešnosti kandidata na izpitu, zlasti o njegovem znanju in sposobnostih na zadevnem področju. Namen teh komentarjev je poleg tega prav dokumentiranje ocene popravljavca glede uspešnosti kandidata in imajo lahko zanj posledice.

Četrtič, Sodišče je razsodilo, da so lahko pisni odgovori, ki jih je na poklicnem izpitu dal kandidat, in morebitni komentarji popravljavca, ki so s temi odgovori povezani, predmet preverjanja, zlasti glede njihove točnosti in nujnosti njihovega shranjevanja v smislu člena 6(1)(d) in (e) Direktive 95/46/ES, in so lahko predmet popravka ali izbrisa na podlagi člena 12(b) te direktive. To, da ima kandidat na podlagi člena 12(a) te direktive pravico do dostopa do teh odgovorov in komentarjev, služi cilju te direktive, ki je zagotavljanje varstva pravice do zasebnega življenja tega kandidata pri obdelavi podatkov, ki se nanj nanašajo, in to ne glede na to, ali ima navedeni kandidat tako pravico do dostopa tudi na podlagi nacionalne ureditve, ki se uporablja za izpitni postopek. Vendar je Sodišče poudarilo, da pravici do dostopa in popravka iz člena 12(a) in (b) Direktive 95/46/ES ne zajemata izpitnih vprašanj, ki kot taka niso osebni podatki kandidata.

Sodišče je na podlagi teh elementov ugotovilo, da so v okoliščinah, kakršne so bile te v postopku v glavni stvari, pisni odgovori, ki jih je na poklicnem izpitu dal kandidat, ter morebitni komentarji popravljavca, ki so s temi odgovori povezani, osebni podatki v smislu člena 2(a) Direktive 95/46/ES.

3. Pojem „obdelava osebnih podatkov“

Sodba z dne 6. novembra 2003 (občna seja), Lindqvist (C-101/01, EU:C:2003:596)

B. Lindqvist, prostovoljna delavka v župniji protestantske cerkve na Švedskem, je na svojem zasebnem računalniku izdelala spletne strani in na njih objavila osebne podatke več oseb, ki so tako kot ona prostovoljno delale v navedeni župniji. B. Lindqvist je bilo naloženo plačilo globe, ker je uporabila osebne podatke v okviru avtomatske obdelave, ne da bi to prej pisno prijavila švedskemu Datainspektion (javni organ za varstvo računalniško prenesenih podatkov), ker jih je brez dovoljenja prenesla v tretje države in ker je obdelovala občutljive osebne podatke.

Göta hovrätt (pritožbeno sodišče, Švedska) je v okviru pritožbe, ki jo je B. Lindqvist vložila pri njem proti tej odločbi, Sodišču predložilo vprašanja za predhodno odločanje, da bi ugotovilo, ali je B. Lindqvist opravila „obdelavo osebnih podatkov v celoti ali delno z avtomatskimi sredstvi“ v smislu Direktive 95/46/ES.

Sodišče je ugotovilo, da je navedba različnih oseb na spletni strani, katerih prepoznavnost je omogočena z navedbo imena ali z drugimi sredstvi, na primer z navedbo telefonske številke ali informacij v zvezi z njihovimi delovnimi razmerami in preživljanjem prostega časa, „obdelava osebnih podatkov v celoti ali delno z avtomatskimi sredstvi“ v smislu te direktive (točka 27 in točka 1 izreka). Taka obdelava osebnih podatkov za opravljanje prostovoljnih ali verskih dejavnosti namreč ne spada k nobeni od izjem od področja uporabe Direktive, saj ne spada ne v kategorijo dejavnosti, katerih predmet je javna varnost, ne v kategorijo popolnoma osebnih ali domačih dejavnosti, ki ne spadajo na področje uporabe Direktive (točke 38, od 43 do 48 in točka 2 izreka).

Sodba z dne 13. maja 2014 (veliki senat), Google Spain in Google (C-131/12, EU:C:2014:317)

Španski državljani leta 2010 pri Agencia Española de Protección de Datos (španska agencija za varstvo podatkov, v nadaljevanju: AEPD) vložil pritožbo proti družbi La Vanguardia Ediciones SL, ki izdaja dnevnik z veliko naklado v Španiji, ter proti družbama Google Spain in Google. Ta oseba je trdila, da če internetni uporabnik v iskalnik skupine Google vpiše njeno ime, se v seznamu zadetkov prikažejo povezave na dve strani dnevnika družbe La Vanguardia iz leta 1998, na katerih je bilo med drugim objavljeno obvestilo o nepremičninski dražbi, ki je bila organizirana po rubežu za poplačilo njenih dolgov. Ta oseba je zahtevala, prvič, naj se družbi La Vanguardia naloži, naj navedeni strani izbriše ali spremeni tako, da osebni podatki te osebe ne bodo več prikazani, ali uporabi nekatera orodja iskalnikov za zaščito teh podatkov. Drugič, zahtevala je, naj se družbi Google Spain ali Google Inc. naloži, naj izbriše ali prekrije njene osebne podatke, tako da ne bodo več prikazani v zadetkih iskanja in v povezavah družbe La Vanguardia.

AEPD je zavrnila pritožbo, vloženo proti družbi Vanguardia, ker je menila, da je izdajatelj zakonito objavil zadevne informacije, ugodila pa je pritožbi proti družbama Google Spain in Google ter tema družbama naložila, da sprejmeta potrebne ukrepe, da podatke odstranita s svojega seznama in v prihodnje onemogočita dostop. Navedeni družbi sta vložili tožbi pri Audiencia Nacional (osrednje sodišče, Španija), da bi dosegli razglasitev ničnosti odločbe AEPD, zato je špansko sodišče Sodišču predložilo vrsto vprašanj.

Tako je imelo Sodišče priložnost pojasniti pojem „obdelava osebnih podatkov“ na internetu z vidika Direktive 95/46/ES.

Tako je Sodišče razsodilo, da dejavnost iskalnika, ki poišče informacije, ki jih objavijo ali postavijo na internet tretje osebe, jih samodejno indeksira, začasno shrani in končno da na voljo internetnim uporabnikom po prednostnem vrstnem redu, šteje za obdelavo osebnih podatkov, če te informacije vsebujejo osebne podatke (točke 1 izreka). Sodišče je poleg tega spomnilo, da je treba postopke iz Direktive šteti za obdelavo, tudi če se nanašajo izključno na informacije, ki so že objavljene v medijih. Ta direktiva bi zaradi splošne izjeme od njene uporabe v tem primeru v veliki meri izgubila smisel (točki 29 in 30).

4. Pogoji zakonitosti obdelave osebnih podatkov z vidika člena 7 Direktive št. 95/46/ES

Sodba z dne 16. decembra 2008 (veliki senat), Huber (C-524/06, EU:C:2008:724)¹⁸

Zvezni urad za migracije in begunce (Bundesamt für Migration und Flüchtlinge, Nemčija) je upravljal centralni register tujcev, v katerem so bili zbrani nekateri osebni podatki tujcev, ki na nemškem ozemlju prebivajo več kot tri mesece. Register se je uporabljal za statistične namene in pri izvajanju pristojnosti varnostnih služb, policije in sodnih organov na področju pregona in preiskav v zvezi s kaznivimi ravnanji ali ogrožanjem javne varnosti.

H. Huber, avstrijski državljan, se je leta 1996 naselil v Nemčiji, da bi tam opravljal poklic neodvisnega zavarovalnega zastopnika. H. Huber je zahteval izbris podatkov, ki se v zadevnem registru nanašajo nanj, ker je menil, da je zaradi obdelave teh podatkov diskriminiran, in sicer zato, ker za nemške državljane taka zbirka podatkov ne obstaja.

V teh okoliščinah je Oberverwaltungsgericht für das Land Nordrhein-Westfalen (višje upravno sodišče dežele Severno Porenje - Vestfalija, Nemčija), ki mu je bil spor predložen, Sodišču predložilo vprašanja v zvezi z združljivostjo obdelave osebnih podatkov, ki se je izvajala v zadevnem registru, s pravom Unije.

Sodišče je najprej opozorilo, da pravica do prebivanja državljana Unije na ozemlju države članice, v kateri ni državljan, ni brezpogojna, temveč lahko zanjo veljajo omejitve. Zato je uporaba registra za podporo organom, pristojnim za izvajanje predpisov o pravici do prebivanja, načeloma legitimna in glede na naravo registra združljiva s prepovedjo diskriminacije na podlagi državljanstva iz člena 12, prvi odstavek, ES (postal člen 18, prvi odstavek, PDEU). Vendar sme tak register vsebovati samo informacije, ki so nujne za ta namen v smislu Direktive o varstvu osebnih podatkov (točke 54, 58 in 59).

Sodišče je glede pojma nujnosti obdelave v smislu člena 7(e) Direktive 95/46/ES najprej opozorilo, da gre za avtonomen pojem prava Unije, ki ga je treba razlagati tako, da popolnoma ustreza namenu Direktive 95/46/ES, kot je opredeljen v členu 1(1) te direktive. Nato je ugotovilo, da je sistem obdelave osebnih podatkov v skladu s pravom Unije, če vsebuje samo podatke, ki so nujni, da lahko navedeni organi izvajajo te predpise, in če njegova centraliziranost omogoča učinkovitejše izvajanje teh predpisov z vidika pravice do prebivanja državljanov Unije, ki niso državljani te države članice.

Nikakor ni mogoče šteti, da sta z vidika člena 7(e) Direktive 95/46/ES shranjevanje in obdelava osebnih podatkov, ki so v okviru takega registra navedeni poimensko, nujni za statistične namene (točke 52, 66 in 68).

¹⁸ Ta sodba je bila predstavljena v Letnem poročilu 2008, str. 45.

Poleg tega je Sodišče glede vprašanja uporabe podatkov iz registra za boj proti kriminalu zlasti navedlo, da se ta cilj nanaša na pregon kaznivih in protizakonitih dejanj, ne glede na državljanstvo storilcev. Zato država članica zaradi cilja boja proti kriminalu ne sme razlikovati med položajem svojih državljanov in položajem državljanov Unije, ki niso državljani te države članice in ki prebivajo na njenem ozemlju. Različno obravnavanje teh državljanov in državljanov Unije – ki je bilo zaradi boja proti kriminalu uvedeno s sistematično obdelavo osebnih podatkov, ki se nanašajo le na državljane Unije, ki niso državljani zadevne države članice – torej pomeni diskriminacijo, ki je prepovedana s členom 12, prvi odstavek, ES (točke od 78 do 80).

Sodba z dne 24. novembra 2011, ASNEF in FECEMD (C-468/10 in C-469/10, EU:C:2011:777)

Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) in Federación de Comercio Electrónico y Marketing Directo (FECEMD) sta pri Tribunal Supremo (Španija) vložili tožbo v upravnem sporu zoper več členov kraljeve uredbe 1720/2007, s katero se izvaja sistemski zakon 15/1999 za prenos Direktive 95/46/ES.

ASNEF in FECEMD sta zlasti menili, da špansko pravo za dovolitev obdelave osebnih podatkov – kadar ni privolitve zadevne osebe – dodaja pogoj, ki ni določen v Direktivi 95/46/ES, s tem, da zahteva, da so navedeni podatki „iz javno dostopnih virov“, kot so naštetih v členu 3(j) sistema zakona 15/1999. V zvezi s tem sta trdili, da ta zakon in kraljeva uredba 1720/2007 omejujeta obseg člena 7(f) Direktive 95/46/ES, s katerim je za obdelavo osebnih podatkov, kadar ni privolitve zadevne osebe, določen pogoj, ki se veže samo na zakonite interese, za katere si prizadeva upravljavec ali tretja stranka ali stranke, ki so jim osebni podatki posredovani.

Sodišče je v zvezi s tem najprej navedlo, da je v členu 7 Direktive 95/46/ES določen izčrpen in taksativen seznam primerov, v katerih je mogoče šteti, da je obdelava osebnih podatkov dopustna ob neobstoju privolitve zadevne osebe. Zato države članice na podlagi člena 5 navedene direktive ne smejo dodati drugih načel glede zakonitosti obdelave osebnih podatkov, kot so tista iz člena 7, niti z dodatnimi zahtevami spremeniti obsega načel, določenih v navedenem členu 7. Člen 5 namreč državam članicam dopušča samo, da v mejah poglavja II navedene direktive in torej člena 7 natančneje določijo pogoje, pod katerimi je obdelava osebnih podatkov zakonita (točke 30, 32 in 33).

Natančneje, države članice lahko za izvedbo potrebnega tehtanja zadevnih nasprotujočih si pravic in interesov, določenega v členu 7(f) navedene direktive, določijo vodilna načela. Upoštevajo lahko tudi to, da je teža posega v temeljne pravice osebe, na katero se navedena obdelava nanaša, lahko različna glede na to, ali so ti podatki že v javno dostopnih virih ali ne (točki 44 in 46).

Vendar je Sodišče ugotovilo, da če nacionalna zakonodaja obdelave nekaterih vrst osebnih podatkov ne dovoljuje, tako da za te vrste dokončno določa izid tehtanja nasprotujočih si pravic in interesov, ne da bi omogočala drugačen izid zaradi posebnih okoliščin konkretnega primera, ne gre za natančnejšo določitev v smislu člena 5 Direktive 95/46/ES. Zato je Sodišče razsodilo, da člen 7(f) Direktive 95/46/ES nasprotuje temu, da država članica kategorično in na splošno izključi možnost obdelave za nekatere vrste osebnih podatkov, ne da bi omogočila tehtanje zadevnih nasprotujočih si pravic in interesov v posebnem primeru (točki 48 in 49).

Sodba z dne 19. oktobra 2016, Breyer (C-582/14, EU:C:2016:779)

Sodišče je v tej sodbi (glej tudi razdelek II.2, naslovljen „Pojem ‚Osebni podatki‘“) odločilo tudi o vprašanju, ali člen 7(f) Direktive 95/46/ES nasprotuje določbi nacionalnega prava, v skladu s katero lahko ponudnik storitev spletnih medijev osebne podatke, ki se nanašajo na nekega uporabnika, brez privolitve uporabnika zbira in uporabi, samo če je to potrebno, da se zadevnemu uporabniku omogoča in

zaračunava konkretni dostop do spletnih medijev, in v skladu s katero cilj zagotavljanja splošnega delovanja spletnih medijev ne upravičuje uporabe podatkov po koncu postopka dostopa do spletnega medija.

Sodišče je razsodilo, da člen 7(f) Direktive 95/46/ES nasprotuje zadevni zakonodaji. V skladu s to določbo je namreč obdelava v smislu te določbe zakonita, če je potrebna zaradi zakonitih interesov, za katere si prizadeva upravljavec ali tretja stranka ali stranke, ki so jim osebni podatki posredovani, razen kadar nad takimi interesi prevladajo temeljne pravice in svoboščine posameznika, na katerega se osebni podatki nanašajo. V obravnavani zadevi pa je bila z nemško zakonodajo kategorično in na splošno izključena možnost za nekatere vrste osebnih podatkov, da se obdelajo, ne da bi omogočila tehtanje zadevnih nasprotujočih si pravic in interesov v posebnem primeru. S tem je bil nezakonito zmanjšan obseg tega načela, določenega v členu 7(f) Direktive 95/46/ES, ker je bilo izključeno, da je cilj zagotavljanja splošnega delovanja teh spletnih medijev lahko predmet tehtanja v primerjavi z interesi ali s temeljnimi pravicami in svoboščinami uporabnikov (točke od 62 do 64 in točka 2 izreka).

Sodba z dne 4. maja 2017, Rīgas satiksme (C-13/16, EU:C:2017:336)

Ta zadeva se je nanašala na spor med latvijsko nacionalno policijo in Rīgas satiksme, avtobusno družbo mesta Riga, glede zahteve za posredovanje podatkov za identifikacijo povzročitelja nesreče. V obravnavani zadevi je prišlo do prometne nesreče, v kateri je voznik taksija svoje vozilo ustavil ob robu ceste. Ko je mimo tega taksija pripeljal avtobus družbe Rīgas satiksme, je potnik, ki je sedel na zadnjem sedežu navedenega taksija, odprl vrata, ki so oplazila in poškodovala avtobus. Družba Rīgas satiksme je za vložitev civilne tožbe od nacionalne policije med drugim zahtevala posredovanje podatkov za identifikacijo povzročitelja nesreče. Policija je zavrnila posredovanje identifikacijske številke in naslova potnika ter dokumentov z zvezi z izjavami oseb, ki so bile vpletene v nesrečo, s pojasnilom, da je mogoče dokumente v zvezi z upravnim postopkom, ki se konča z izrekom sankcij, posredovati samo strankam tega postopka, glede naslova in identifikacijske številke pa je bilo pojasnjeno, da je z zakonom o varstvu osebnih podatkov prepovedano razkritje takih informacij o posameznikih.

V teh okoliščinah je Augstākās tiesas Administratīvo lietu departaments (vrhovno sodišče, oddelek za upravne zadeve, Latvija) odločilo, da Sodišču predloži vprašanje, ali je s členom 7(f) Direktive 95/46/ES naložena obveznost posredovanja osebnih podatkov tretji stranki, da bi se ji omogočila vložitev odškodninske tožbe pri civilnem sodišču zaradi škode, ki jo je povzročila oseba, na katero se nanaša varstvo teh podatkov, in ali lahko to, da je ta oseba mladoletna, vpliva na razlago te določbe.

Sodišče je razsodilo, da je treba člen 7(f) Direktive 95/46/ES razlagati tako, da ne nalaga obveznosti posredovanja osebnih podatkov tretji stranki, da bi se ji omogočila vložitev odškodninske tožbe pri civilnem sodišču zaradi škode, ki jo je povzročila oseba, na katero se nanaša varstvo teh podatkov. Vendar ta določba ne bi nasprotovala takemu posredovanju, če bi bilo to opravljeno na podlagi nacionalnega prava ob spoštovanju pogojev iz te določbe (točki 27 in 34 ter izrek).

Sodišče je v tem okviru s pridržkom preveritev, ki jih je moralo v zvezi s tem opraviti predložitveno sodišče, ugotovilo, da v okoliščinah, kakršne so v postopku v glavni stvari, ni upravičeno oškodovancu zavrniti posredovanja osebnih podatkov, potrebnih za vložitev odškodninske tožbe proti storilcu škode, ali, odvisno od primera, osebam, ki uresničujejo starševske pravice, ker bi bil ta storilec mladoleten (točka 33).

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

V sporu o glavni stvari je P. Puškár pri Najvyšší súd Slovenskej republiky (vrhovno sodišče Slovaške republike) zahteval, naj se Finančné riaditeľstvo (direktorat za finance), vsem njemu podrejenim davčnim

uradom in Kriminálny úrad finančnej správy (urad za boj proti finančnemu kriminalu) naloži prepoved vpisa njegovoga imena na seznam oseb, ki jih direktorat za finance šteje za osebe s fiktivnimi vodstvenimi položaji, ki ga je ta direktorat oblikoval v okviru pobiranja davkov, posodabljata pa ga direktorat za finance in urad za boj proti finančnemu kriminalu (v nadaljevanju: sporni seznam). Poleg tega je zahteval, naj se s teh seznamov in informacijskega sistema finančne uprave izbriše vsaka navedba v zvezi z njim.

Najvyšší súd je v teh okoliščinah Sodišču med drugim predložilo vprašanje, ali je mogoče pravico do spoštovanja zasebnega in družinskega življenja, stanovanja ter komunikacij, določeno v členu 7 Listine, ter pravico do varstva osebnih podatkov, določeno v členu 8 Listine, razlagati tako, da nasprotujejo temu, da država članica brez soglasja zadevnih oseb oblikuje sezname osebnih podatkov za namen pobiranja davkov, tako da bi bilo pridobivanje osebnih podatkov, ki ga javni organi izvajajo z namenom boja proti davčni goljufiji, tvegano početje.

Sodišče je ugotovilo, da člen 7(e) Direktive 95/46/ES ne nasprotuje temu, da organi države članice brez soglasja zadevnih oseb obdelujejo osebne podatke za namene pobiranja davkov in boja proti davčnim goljufijam, kot so to storili z oblikovanjem seznama oseb, kakršen je sporni seznam iz zadeve v glavni stvari, če so ti organi, prvič, v skladu z nacionalno zakonodajo pooblaščen za izvajanje nalog v javnem interesu v smislu te določbe, če je oblikovanje spornega seznama in vključitev imen zadevnih oseb nanj dejansko primerno in potrebno za uresničitev zastavljenih ciljev ter če obstajajo zadostni indici za domnevo, da so zadevne osebe utemeljeno uvrščene na ta seznam, in drugič, če so izpolnjeni vsi pogoji za zakonitost te obdelave osebnih podatkov, določeni z Direktivo 95/46/ES (točka 117 in točka 3 izreka).

Sodišče je v zvezi s tem navedlo, da mora nacionalno sodišče preveriti, ali je oblikovanje spornega seznama potrebno za izvajanje nalog v javnem interesu iz zadeve v glavni stvari, ob upoštevanju zlasti natančnega cilja oblikovanja spornega seznama, pravnih posledic za osebe, uvrščene na ta seznam, in javnost ter zaupnosti tega seznama. Poleg tega mora nacionalno sodišče ob upoštevanju načela sorazmernosti preveriti, ali je oblikovanje spornega seznama in vključitev imen zadevnih oseb nanj primerno za uresničitev zastavljenih ciljev in ali teh ciljev ni mogoče uresničiti z drugimi, manj omejujočimi ukrepi (točke 111, 112 in 113).

Sodišče je še ugotovilo, da vključitev imena osebe na sporni seznam lahko poseže v nekatere njene pravice. Vpis na ta seznam lahko namreč škoduje njenemu ugledu in vpliva na njen odnos z davčnimi organi. Ta vpis lahko vpliva tudi na domnevo nedolžnosti te osebe, zagotovljeno v členu 48(1) Listine, in v členu 16 Listine določeno svobodo gospodarske pobude pravnih oseb, ki so povezane s fizičnimi osebami, vpisanimi na sporni seznam. Zato je takšen poseg lahko primeren, samo če obstajajo zadostni indici za sum, da ima zadevna oseba fiktivni vodstveni položaj v pravnih osebah, s katerimi se jo povezuje, s čimer onemogoča pobiranje davkov in boj proti davčnim goljufijam (točka 114).

Poleg tega je Sodišče ugotovilo, da če bi v skladu s členom 13 Direktive 95/46/ES obstajali razlogi za omejitev nekaterih pravic iz člena 6 in členov od 10 do 12 te direktive, kot je pravica zadevne osebe do prejetja informacij, bi morala biti taka omejitev potrebna za zaščito interesa, navedenega v odstavku 1 navedenega člena 13, kot je med drugim pomemben gospodarski ali finančni interes v zvezi z davčnimi zadevami, in bi morala temeljiti na zakonskih predpisih (točka 116).

III. Prenos osebnih podatkov v tretje države

Sodba z dne 6. novembra 2003 (občna seja), Lindqvist (C-101/01, EU:C:2003:596)¹⁹

V tej zadevi (glej tudi razdelek II.3, naslovljen „Pojem ‚obdelava osebnih podatkov‘“) je predložitveno sodišče želelo zlasti izvedeti, ali je B. Lindqvist opravila prenos podatkov v tretjo državo v smislu navedene direktive.

Sodišče je razsodilo, da ne gre za „prenos podatkov v tretjo državo“ v smislu člena 25 Direktive 95/46/ES, kadar oseba, ki je v eni od držav članic, na spletno stran, shranjeno pri fizični ali pravni osebi, ki gosti spletišče, na katerem si je mogoče stran ogledati, in ki ima stalno prebivališče ali sedež v isti ali drugi državi članici, vnese osebne podatke in tako omogoči dostop do njih vsakomur, ki se poveže na splet, tudi osebam v tretjih državah (točka 71 in točka 4 izreka).

Ob upoštevanju stanja razvoja spleta v času nastanka Direktive 95/46/ES na eni strani in ne vključitve meril v zvezi z uporabo spleta v poglavje IV te direktive, v katero spada navedeni člen 25, s katerim se zagotavlja nadzor držav članic nad prenosom osebnih podatkov v tretje države in prepoveduje te prenose, če ti ne omogočajo primerne ravni varstva, na drugi strani, namreč ni mogoče predpostaviti, da je nameraval zakonodajalec Skupnosti v pojem „prenos podatkov v tretjo državo“ vnaprej vključiti vnos podatkov na spletno stran, tudi če ti podatki s tem postanejo dostopni osebam iz tretjih držav, ki imajo tehnična sredstva za dostop do njih (točke 63, 64 in 68).

Sodba z dne 6. oktobra 2015 (veliki senat), Schrems (C-362/14, EU:C:2015:650)²⁰

M. Schrems, avstrijski državljan in uporabnik družabnega omrežja Facebook, je pri Data Protection Commissioner (pooblaščenec za varstvo podatkov, Irska) vložil pritožbo, ker je Facebook Ireland osebne podatke svojih uporabnikov prenašal v Združene države in jih hranil na strežnikih v tej državi, kjer so se obdelovali. Po navedbah M. Schremsa pravo in praksa v Združenih državah ne zagotavljata zadostne zaščite podatkov, prenesenih v to državo, pred nadzorom, ki ga tam izvajajo državni organi. Data Protection Commissioner ni želel preučiti te pritožbe, med drugim zato, ker je Komisija v Odločbi 2000/520/ES²¹ ugotovila, da Združene države v okviru sistema „varnega pristana“ (angleško „safe harbour“),²² zagotavljajo ustrezno raven zaščite prenesenih osebnih podatkov.

V teh okoliščinah je High Court (višje sodišče, Irska) pri Sodišču vložilo predlog za razlago člena 25(6) Direktive 95/46/ES, v skladu s katerim lahko Komisija ugotovi, da tretja država zagotavlja ustrezno raven varstva prenesenih podatkov, in v bistvu tudi predlog za ugotovitev veljavnosti Odločbe 2000/520/ES, ki jo je Komisija sprejela na podlagi navedenega člena 25(6) Direktive 95/46/ES.

Sodišče je ugotovilo, da Odločba Komisije v celoti ni veljavna in najprej poudarilo, da mora Komisija, da lahko sprejme tako odločbo, obrazloženo ugotoviti, da zadevna tretja država dejansko zagotavlja raven varstva temeljnih pravic, ki je v bistvenem enaka ravni, zagotovljeni v pravnem redu Unije. Ker pa Komisija v Odločbi 2000/520/ES tega ni storila, člen 1 te odločbe krši zahteve, določene v členu 25(6) Direktive 95/46/ES, razlagane ob upoštevanju Listine, in zato ni veljaven. Načela „varnega pristana“ se namreč uporabljajo zgolj za samocertificirane ameriške organizacije, ki prejemajo osebne podatke iz

¹⁹ Ta sodba je bila predstavljena v Letnem poročilu 2003, str. 67.

²⁰ Ta sodba je bila predstavljena v Letnem poročilu 2015, str. 48.

²¹ Odločba Komisije 2000/520/ES z dne 26. julija 2000 po Direktivi Evropskega parlamenta in Sveta 95/46/ES o primernosti zaščite, ki jo zagotavljajo načela zasebnosti varnega pristana in s tem povezana najpogosteje zastavljena vprašanja, ki jih je izdalo Ministrstvo za trgovino ZDA (UL, posebna izdaja v slovenščini, poglavje 16, zvezek 1, str. 119).

²² Sistem varnega pristana zajema več načel, ki se nanašajo na varstvo osebnih podatkov in ki se jim lahko ameriška podjetja prostovoljno zavežejo.

Unije, ne zahteva pa se, da tudi ameriški javni organi spoštujejo navedena načela. Poleg tega Odločba 2000/520/ES omogoča posege v temeljne pravice oseb, katerih osebni podatki se prenašajo ali bi se lahko prenašali iz Unije v Združene države, ne da bi vsebovala ugotovitev glede tega, ali v Združenih državah obstajajo državni predpisi, katerih namen bi bil omejiti morebitne posege v te pravice in ne da bi omenila obstoj učinkovitega sodnega varstva v primeru takih posegov (točke 82, od 87 do 89 in od 96 do 98 ter izrek).

Sodišče je poleg tega ugotovilo, da člen 3(1) Odločbe 2000/ES ni veljaven, ker nacionalnim nadzornim organom odvzema pooblastila, ki jih imajo na podlagi člena 28 Direktive 95/46/ES, kadar posameznik navaja elemente, ki lahko izpodbijejo skladnost odločbe Komisije, v kateri je ta ugotovila, da tretja država zagotavlja ustrezno raven varstva, z varstvom zasebnega življenja ter temeljnih svoboščin in pravic posameznikov (točke od 102 do 104). Sodišče je nazadnje ugotovilo, da neveljavnost členov 1 in 3 Odločbe 2002/520/ES vpliva na veljavnost te odločbe v celoti.

V zvezi z nezmožnostjo utemeljitve takega posega je Sodišče najprej opozorilo, da mora predpis Unije, ki pomeni poseg v temeljne pravice, zagotovljene v členih 7 in 8 Listine, določati jasna in natančna pravila, ki urejajo obseg in uporabo ukrepa ter določajo minimalne zahteve, tako da imajo osebe, za katerih osebne podatke gre, zadostna jamstva, ki omogočajo učinkovito varovanje njihovih podatkov pred zlorabo ter pred vsakršnim nezakonitim dostopom in uporabo teh podatkov. Potreba po takih jamstvih je toliko pomembnejša, če so osebni podatki predmet avtomatske obdelave in obstaja veliko tveganje nezakonitega dostopa do teh podatkov (točka 91).

Poleg tega in predvsem, varstvo temeljne pravice do spoštovanja zasebnega življenja na ravni Unije zahteva, da se odstopanja od varstva osebnih podatkov in njegove omejitve določijo v mejah tega, kar je nujno potrebno (točka 92). Torej ni zgolj na nujno potrebno omejena ureditev, ki splošno dovoljuje hrambo vseh osebnih podatkov vseh posameznikov, katerih podatki so bili preneseni iz Unije, ne da bi se uporabljalo kakršno koli razlikovanje, omejitev ali izjema glede na cilj, ki se ga poskuša doseči, in ne da bi bilo določeno objektivno merilo, ki bi omogočalo dostop javnih organov do podatkov in poznejšo uporabo teh podatkov samo v namene, ki so natančno določeni, strogo omejeni in bi lahko utemeljevali poseg, ki ga pomenita dostop in uporaba teh podatkov (točka 93). Natančneje, ureditev, ki javnim organom omogoča splošen dostop do vsebine elektronskih komunikacij, pomeni poseg v bistvo temeljne pravice do spoštovanja zasebnega življenja. Poleg tega ureditev, ki ne določa nobene možnosti, da bi posameznik lahko uporabil pravna sredstva za pridobitev dostopa do osebnih podatkov, ki se nanj nanašajo, ali dosegel popravilo ali izbris takih podatkov, posega v bistvo temeljne pravice do učinkovitega sodnega varstva, določene v členu 47 Listine (točki 94 in 95).

Mnenje 1/15 (Sporazum PNR EU-Kanada) z dne 26. julija 2017 (veliki senat) (EU:C:2017:592)

Sodišče se je 26. julija 2017 prvič izreklo o združljivosti osnutka mednarodnega sporazuma z Listino Evropske unije o temeljnih pravicah in, natančneje, z določbami v zvezi s spoštovanjem zasebnega življenja in varstvom osebnih podatkov.

Evropska unija in Kanada sta se dogovorili za sporazum o prenosu in obdelavi podatkov iz evidence podatkov o potnikih (sporazum PNR), ki je bil podpisan leta 2014. Svet Evropske unije je Evropski parlament pozval, naj ta sporazum odobri, ta pa je odločil, da se zadeva predloži Sodišču, da bi se ugotovilo, ali je predvideni sporazum v skladu s pravom Unije.

Predvideni sporazum omogoča sistematičen in stalen prenos podatkov iz PNR o vseh letalskih potnikih kanadskemu organu za njihovo uporabo in hrambo ter njihov morebiten poznejši prenos drugim organom in drugim tretjim državam, s ciljem boja proti terorističnim in drugim hudim mednarodnim kaznivim dejanjem. Predvideni sporazum v ta namen med drugim določa petletno hrambo podatkov in posebne zahteve glede varnosti in celovitosti podatkov iz PNR, kot je takojšnje prikritje občutljivih

podatkov, ter pravico do dostopa do podatkov, do popravka in izbrisa ter možnost vložitve pravnih sredstev v upravnih in sodnih postopkih.

Podatki iz PNR, na katere se nanaša predvideni sporazum, obsegajo med drugim ime ali imena ter kontaktne informacije letalskih potnikov, informacije, potrebne za rezervacijo, kot so predvideni datumi potovanja in načrt potovanja, informacije o vozovnicah, skupine oseb, registriranih pod isto številko rezervacije, informacije o plačilnem sredstvu ali zaračunavanju, informacije o prtljagi in splošne opombe glede potnikov.

Sodišče je v mnenju ugotovilo, da sporazuma PNR ni mogoče skleniti v obstoječi obliki, ker več njegovih določb ni združljivih s temeljnimi pravicami, ki jih priznava Unija.

Sodišče je ugotovilo, da, prvič, tako prenos podatkov iz PNR iz Unije kanadskemu pristojnemu organu kot okvir pogojev, o katerem se je Unija dogovorila s Kanado, v zvezi s pogoji za hrambo teh podatkov, njihovo uporabo in za njihove morebitne nadaljnje prenose drugim kanadskim organom, Europolu, Eurojustu, pravosodnim ali policijskim organom držav članic ali celo organom drugih tretjih držav, pomenita poseganje v pravico, zagotovljeno s členom 7 Listine. Ti ravnanji pomenita tudi poseganje v temeljno pravico do varstva osebnih podatkov, zagotovljeno s členom 8 Listine, saj gre pri njiju za obdelavo osebnih podatkov (točki 125 in 126).

Poleg tega je poudarilo, da tudi če se zdi, da nekateri podatki iz PNR, obravnavani ločeno, ne morejo razkriti pomembnih informacij o zasebnem življenju zadevnih oseb, lahko navedeni podatki, obravnavani skupaj, vseeno razkrijejo popoln načrt potovanja, potovalne navade, razmerja med dvema ali več osebami in informacije o finančnem položaju letalskih potnikov, njihove prehranske navade ali njihovo zdravstveno stanje ter bi lahko celo zagotovili občutljive informacije o teh potnikih, kot so opredeljene v členu 2(e) predvidenega sporazuma (informacije, ki razkrivajo rasno ali etnično poreklo, politična ali verska prepričanja in podobno) (točka 128).

Sodišče je v zvezi s tem ugotovilo, da bi bilo zadevna poseganja sicer mogoče upravičiti z uresničevanjem cilja splošnem interesu (zagotavljanje javne varnosti v okviru boja proti terorističnim in hudim mednarodnim kaznivim dejanjem), vendar več določb sporazuma ni omejenih na tisto, kar je nujno potrebno in ne določajo jasnih in natančnih pravil.

Sodišče je posebej ugotovilo, da bi bila za prenos občutljivih podatkov v Kanado, ob upoštevanju nevarnosti, da bi bila obdelava podatkov v nasprotju z načelom prepovedi diskriminacije, potrebna natančna in posebej trdna utemeljitev z razlogi, ki niso zaščita javne varnosti pred terorizmom in hudimi mednarodnimi kaznivimi dejanji. V obravnavanem primeru pa taka utemeljitev ni podana. Sodišče je zato presodilo, da določbe sporazuma o prenosu občutljivih podatkov v Kanado ter o obdelavi in hrambi teh podatkov niso združljive s temeljnimi pravicami (točki 165 in 232).

Drugič, Sodišče je menilo, da nadaljnja hramba podatkov iz PNR o vseh letalskih potnikih po njihovem odhodu iz Kanade, ki je omogočena s sporazumom, ni omejena na tisto, kar je nujno potrebno. Glede letalskih potnikov, za katere tveganje v zvezi s terorizmom in hudimi mednarodnimi kaznivimi dejanji ni bilo ugotovljeno ob njihovem prihodu v Kanado in do njihovega odhoda iz te države, ni razvidno, da bi po njihovem odhodu obstajala povezava, tudi če le posredna, med njihovimi podatki iz PNR in ciljem predvidenega sporazuma, ki bi upravičevala hrambo teh podatkov. Vendar je dopustno hraniti podatke iz PNR potnikov, če se ugotovijo objektivni elementi, na katerih podlagi je mogoče šteti, da bi lahko ti potniki tudi po svojem odhodu iz Kanade pomenili tveganje z vidika boja proti terorizmu in hudim mednarodnim kaznivim dejanjem, tudi za obdobje petih let (točke od 205 do 207 in 209).

Tretjič, Sodišče je ugotovilo, da temeljna pravica do spoštovanja zasebnega življenja, določena v členu 7 Listine Evropske unije o temeljnih pravicah, pomeni, da se lahko zadevna oseba prepriča, da se njeni

osebni podatki obdelujejo natančno in zakonito. Da bi ta oseba lahko opravila potrebna preverjanja, mora imeti pravico do dostopa do obdelovanih podatkov, ki se nanjo nanašajo.

V zvezi s tem je poudarilo, da je v predvidenem sporazumu pomembno, da so letalski potniki obveščeni o prenosu njihovih podatkov iz evidence podatkov o potnikih v zadevno tretjo državo in o obdelavi teh podatkov od takrat, ko to razkritje ne more ogroziti preiskav, ki jih opravljajo javni organi, na katere se predvideni sporazum nanaša. Taka informacija je dejansko nujna, da se lahko letalskim potnikom omogoči uveljavljanje njihovih pravic, da zahtevajo dostop do podatkov, ki se nanje nanašajo, in po potrebi njihov popravek ter da v skladu s členom 47, prvi odstavek, Listine vložijo učinkovito pravno sredstvo pred sodiščem.

Tako je v primerih, v katerih so podani objektivni elementi, ki upravičujejo uporabo podatkov potnikov za boj proti terorizmu in hudim mednarodnim kaznivim dejanjem in zahtevajo predhodno dovoljenje sodnega ali neodvisnega upravnega organa, individualna obvestitev letalskih potnikov nujna. Enako velja, če se podatki iz PNR o letalskih potnikih razkrijejo drugim javnim organom ali posameznikom. Vendar lahko do take obvestitve pride šele po tem, ko ta ne more ogroziti preiskav, ki jih opravljajo javni organi, na katere se predvideni sporazum nanaša (točke 219, 220, 223 in 224).

IV. Varstvo osebnih podatkov na internetu

1. Pravica do ugovora zoper obdelavo osebnih podatkov („pravica biti pozabljen“)

Sodba z dne 13. maja 2014 (veliki senat), Google Spain in Google (C-131/12, EU:C:2014:317)

Sodišče je v tej sodbi (glej razdelek II.3, naslovljen „Pojem ‚obdelava osebnih podatkov‘“) natančneje pojasnilo vsebino pravic do dostopa in do ugovora zoper obdelavo osebnih podatkov na internetu, določenih z Direktivo 95/46/ES.

Tako je Sodišče pri odločanju o obsegu odgovornosti upravljavca internetnega iskalnika v bistvu razsodilo, da mora ta zaradi spoštovanja pravic do dostopa in do ugovora, zagotovljenih s členoma 12(b) in 14, prvi odstavek, (a), Direktive 95/46/ES, in če so pogoji iz teh določb dejansko izpolnjeni, s seznama zadetkov, ki se prikaže po iskanju, opravljenem na podlagi imena osebe, odstraniti povezave na spletne strani, ki jih objavijo tretje osebe in ki vsebujejo informacije, ki se nanašajo na to osebo. Sodišče pojasnjuje, da ta obveznost obstaja, tudi če to ime ali te informacije niso predhodno ali sočasno izbrisane s teh spletnih strani in tudi če je – če gre za tak primer – njihova objava na navedenih straneh sama po sebi zakonita (točka 88 in točka 3 izreka).

Poleg tega je Sodišče, ki mu je bilo postavljeno vprašanje, ali lahko zadevna oseba na podlagi Direktive zahteva, naj se s takega seznama zadetkov odstranijo povezave na spletne strani, ker želi, da bi bile te informacije v zvezi z njo po določenem času „pozabljene“, najprej navedlo, da celo izvorno zakonita obdelava točnih podatkov lahko sčasoma postane nezdržljiva s to direktivo, če ti podatki niso več potrebni za namene, zaradi katerih so bili zbrani ali obdelani, med drugim, če so neprimerni, neustrezni ali ne več ustrezni ali pretirani glede na te namene in pretečen čas (točka 93). Če je torej po tem, ko je zadevna oseba vložila zahtevo, ugotovljeno, da zdaj to, da so na seznam vključene te povezave, ni združljivo z Direktivo, je treba informacije in zadevne povezave navedenega seznama izbrisati (točka 94). V teh okoliščinah ugotovitev obstoja pravice zadevne osebe do tega, da informacija, ki se nanaša nanjo, ni več povezana z njenim imenom v seznamu zadetkov, ni odvisna od tega, ali vključitev zadevne informacije na seznam zadetkov zadevni osebi povzroča škodo (točka 96 in točka 4 izreka).

Sodišče je nazadnje pojasnilo, da lahko zadevna oseba v skladu s temeljnimi pravicami, ki jih ima na podlagi členov 7 in 8 Listine, zahteva, da zadevna informacija ni več na voljo splošni javnosti prek vključitve na tak seznam zadetkov, zato imajo te pravice načeloma prednost ne le nad gospodarskim interesom upravljavca iskalnika, ampak tudi nad interesom te javnosti, da navedeno informacijo najde z iskanjem na podlagi imena te osebe. Vendar ne bi bilo tako, če bi se izkazalo, da je iz posebnih razlogov, kot je vloga navedene osebe v javnem življenju, poseg v njene temeljne pravice upravičen zaradi prevladujočega interesa navedene javnosti, da ima prek te vključitve dostop do zadevne informacije (točka 97 in točka 4 izreka).

2. Obdelava osebnih podatkov in pravice intelektualne lastnine

*Sodba z dne 29. januarja 2008 (veliki senat), Promusicae (C-275/06, EU:C:2008:54)*²³

Promusicae, špansko neprofitno združenje, ki povezuje proizvajalce in založnike glasbenih in avdiovizualnih posnetkov, je pri španskih sodiščih vložilo zahtevo, naj se družbi Telefónica de España SAU (gospodarska družba, ki se ukvarja zlasti s ponujanjem dostopa do interneta) naloži razkritje imen in naslovov določenih oseb, ki jim slednja zagotavlja dostop do interneta in katerih IP-naslov ter datum in ura povezave so bili znani. V skladu z navedbami združenja Promusicae so te osebe uporabljale program izmenjave arhivov, tako imenovani „peer-to-peer“ ali „P2P“ (pregledno, neodvisno in decentralizirano sredstvo za izmenjavo datotek, opremljeno z naprednimi orodji za iskanje in prenašanje), in iz datoteke za skupno uporabo na njihovem osebnem računalniku omogočale dostop do zvočnih zapisov, katerih pravice materialnega izkoriščanja imajo člani združenja Promusicae. To združenje je torej zahtevalo posredovanje teh informacij, da bi lahko zoper zadevne osebe sprožilo civilne postopke.

V teh okoliščinah je Mercantil nº 5 de Madrid (trgovinsko sodišče št. 5 v Madridu, Španija) Sodišču predložilo vprašanje, ali evropska zakonodaja državam članicam nalaga, da za zagotovitev učinkovitega varstva avtorske pravice določijo obveznost posredovanja osebnih podatkov v okviru civilnega postopka.

Po mnenju Sodišča je navedeni predlog za sprejetje predhodne odločbe zadeval vprašanje potrebne uskladitve zahtev, povezanih z varstvom različnih temeljnih pravic, in sicer, po eni strani, pravice do spoštovanja zasebnega življenja, in po drugi strani, pravic do varstva lastnine in do učinkovitega pravnega sredstva.

Sodišče je v zvezi s tem ugotovilo, da Direktiva 2000/31/ES o nekaterih pravnih vidikih storitev informacijske družbe, zlasti elektronskega poslovanja na notranjem trgu (Direktiva o elektronskem poslovanju),²⁴ Direktiva 2001/29/ES o usklajevanju določenih vidikov avtorske in sorodnih pravic v informacijski družbi,²⁵ Direktiva 2004/48/ES o uveljavljanju pravic intelektualne lastnine²⁶ in Direktiva 2002/58/ES državam članicam ne nalagajo, da v primeru, kot je ta v postopku v glavni stvari, določijo obveznost posredovanja osebnih podatkov, da bi se zagotovilo učinkovito varstvo avtorske pravice v okviru civilnega sodnega postopka. Vendar pa pravo Unije od navedenih držav zahteva, da ob prenosu teh direktiv pazijo, da se oprejo na takšno razlago teh direktiv, ki omogoča zagotovitev pravnega ravnovesja med temeljnimi pravicami, varovanimi s pravnim redom Unije. Dalje, organi in sodišča držav članic morajo ob uporabi ukrepov za prenos teh direktiv ne zgolj razlagati nacionalno pravo v skladu s temi direktivami, temveč tudi paziti, da se ne oprejo na tako razlago teh direktiv, ki bi bila v nasprotju z

²³ Ta sodba je bila predstavljena v Letnem poročilu 2008, str. 41.

²⁴ Direktiva 2000/31/ES Evropskega parlamenta in Sveta z dne 8. junija 2000 o nekaterih pravnih vidikih storitev informacijske družbe, zlasti elektronskega poslovanja na notranjem trgu (Direktiva o elektronskem poslovanju) (UL, posebna izdaja v slovenščini, poglavje 13, zvezek 25, str. 399).

²⁵ Direktiva 2001/29/ES Evropskega parlamenta in Sveta z dne 22. maja 2001 o usklajevanju določenih vidikov avtorske in sorodnih pravic v informacijski družbi (UL, posebna izdaja v slovenščini, poglavje 17, zvezek 1, str. 230).

²⁶ Direktiva Evropskega parlamenta in Sveta 2004/48/ES z dne 29. aprila 2004 o uveljavljanju pravic intelektualne lastnine (UL, posebna izdaja v slovenščini, poglavje 17, zvezek 2, str. 32).

navedenimi temeljnimi pravicami ali z drugimi splošnimi načeli prava Unije, kot je načelo sorazmernosti (točka 70 in izrek).

Sodba z dne 24. novembra 2011, Scarlet Extended (C-70/10, EU:C:2011:771)²⁷

Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM) je ugotovila, da internetni uporabniki, ki uporabljajo storitve družbe Scarlet Extended SA, ki je ponudnik dostopa do interneta (v nadaljevanju: Scarlet), s pomočjo omrežij „peer-to-peer“ prek interneta prenašajo dela, ki so navedena v njenem katalogu, ne da bi za to pridobili dovoljenje in plačali nadomestila. Družba SABAM je zadevo predložila nacionalnemu sodišču, in dosegla, da je to na prvi stopnji družbi Scarlet naložilo, naj zagotovi prenehanje kršitve avtorske pravice, tako da svojim strankam onemogoči, da z uporabo programske opreme „peer-to-peer“ kakor koli pošiljajo ali sprejemajo elektronske datoteke z glasbenimi deli iz repertoarja družbe SABAM.

Cour d'appel de Bruxelles (pritožbeno sodišče v Bruslju, Belgija), na katero se je obrnila družba Scarlet, je prekinilo odločanje, da bi Sodišču predložilo predlog za sprejetje predhodne odločbe v zvezi z vprašanjem, ali je taka odredba v skladu z evropskim pravom.

Sodišče je razsodilo, da je treba direktive 95/46/ES, 2000/31/ES, 2001/29/ES, 2002/58/ES in 2004/48/ES, razlagane skupaj in ob upoštevanju zahtev, ki izhajajo iz varstva temeljnih pravic, ki se uporabijo, razlagati tako, da nasprotujejo temu, da se družbi Scarlet odredi vzpostavitev sistema filtriranja vseh elektronskih komunikacij, ki se prenašajo z njenimi storitvami, zlasti z uporabo programske opreme „peer-to-peer“, ki se uporabi brez razlikovanja za vse njene stranke, preventivno, na njene izključne stroške in časovno neomejeno ter s katerim je mogoče v omrežju tega ponudnika ugotoviti pretok elektronskih datotek, ki vsebujejo glasbena, kinematografska ali avdiovizualna dela, o katerih tožeča stranka trdi, da ima v zvezi z njimi pravice intelektualne lastnine, z namenom blokiranja prenosa datotek, katerih izmenjava pomeni kršitev avtorske pravice (točka 54 in izrek).

Po mnenju Sodišča se namreč s tako odredbo ne spoštuje prepoved iz člena 15(1) Direktive 2000/31/ES, da se takemu ponudniku naloži obveznost splošnega nadzora, niti zahteva, da je treba zagotoviti pravično ravnotežje med pravico intelektualne lastnine na eni strani in svobodno gospodarsko pobudo, pravico do varstva osebnih podatkov ter svobodo sprejemanja in širjenja vesti na drugi (točki 40 in 49).

Sodišče je v tem okviru po eni strani ugotovilo, da odredba, s katero je naložena vzpostavitev spornega sistema za filtriranje, vključuje sistematično analizo vseh vsebin in zbiranje ter identifikacijo IP-naslovov uporabnikov, ki pošiljajo nezakonite vsebine prek omrežja, ti naslovi pa so varovani osebni podatki, saj omogočajo natančno identifikacijo teh uporabnikov (točka 51). Po drugi strani pa bi bila lahko z navedeno odredbo kršena svoboda obveščanja, saj obstaja nevarnost, da ta sistem ne bi dovolj dobro razločeval nezakonitih vsebin od zakonitih, tako da bi njegova vzpostavitev lahko onemogočila prenašanje zakonitih vsebin. Ni namreč sporno, da je odgovor na vprašanje, ali je prenos zakonit, odvisen tudi od zakonskih omejitev avtorske pravice, ki se od države članice do države članice razlikujejo. Poleg tega so nekatera dela lahko v nekaterih članicah v prosti uporabi ali pa so jih zadevni avtorji neodplačno dali na razpolago na splet (točka 52).

Zato je Sodišče ugotovilo, da zadevno nacionalno sodišče s sprejetjem odredbe, s katero je bila družbi Scarlet naložena vzpostavitev spornega sistema za filtriranje, ni spoštovalo zahteve, da je treba zagotoviti pravično ravnotežje med pravico intelektualne lastnine na eni strani in svobodno gospodarsko pobudo, pravico do varstva osebnih podatkov ter svobodo sprejemanja in širjenja vesti na drugi (točka 53).

²⁷ Ta sodba je bila predstavljena v Letnem poročilu 2011, str. 34.

Sodba z dne 19. aprila 2012, Bonnier Audio in drugi (C-461/10, EU:C:2012:219)

Högsta domstolen (vrhovno sodišče, Švedska) je pri Sodišču vložilo predlog za predhodno odločanje za razlago direktiv 2002/58/ES in 2004/48/ES v okviru spora med družbami Bonnier Audio AB, Earbooks AB, Norstedts Förlagsgrupp AB, Piratförlaget AB in Storyside AB (v nadaljevanju: Bonnier Audio in druge) ter družbo Perfect Communication Sweden AB (v nadaljevanju: ePhone) glede nasprotovanja zadnjenedene predlogu za izdajo odredbe o razkritju podatkov, ki so ga vložile družba Bonnier Audio in druge.

V obravnavani zadevi so bile družba Bonnier Audio in druge založnice in so imele med drugim izključne pravice do reproduciranja, izdajanja in priobčitve javnosti 27 del v obliki zvočnih knjig. Menile so, da so bile njihove izključne pravice kršene s tem, da je bilo teh 27 del javnosti priobčenih brez njihovega privoljenja prek strežnika FTP („file transfer protocol“), ki omogoča izmenjavo datotek in prenos podatkov med računalniki, povezanimi z internetom. Zato so pri švedskih sodiščih vložile predlog za izdajo odredbe o razkritju imena in naslova osebe, ki uporablja IP-naslov, s katerim naj bi bile zadevne datoteke prenesene.

V teh okoliščinah je Högsta domstolen, pri katerem je bila vložena kasacijska pritožba, Sodišču predložilo vprašanje, ali pravo Unije nasprotuje uporabi nacionalne določbe, ki temelji na členu 8 Direktive 2004/48/ES in ki dovoljuje, da se ponudniku internetnih storitev v civilnem postopku zaradi identifikacije naročnika odredi, naj imetniku avtorske pravice ali njegovemu pravnemu nasledniku razkrije podatke o identiteti naročnika, ki mu je ponudnik internetnih storitev dodelil IP-naslov, ki naj bi bil uporabljen pri kršitvi navedene pravice. Domnevalo se je, da je predlagatelj odredbe zbral dejanske indice o kršitvi avtorske pravice in da je predlagani ukrep sorazmeren.

Sodišče je najprej spomnilo, da člen 8(3) Direktive 2004/48/ES v povezavi s členom 15(1) Direktive 2002/58/ES ne nasprotuje temu, da države članice določijo obveznost, da se osebam zasebnega prava posredujejo osebni podatki, zato da se pred civilnimi sodišči lahko začnejo postopki zaradi kršitev avtorskih pravic, vendar pa tem državam tudi ne nalaga, da morajo določiti tako obveznost. Vendar morajo organi in sodišča držav članic ne zgolj razlagati nacionalno pravo v skladu s temi direktivami, temveč tudi paziti, da se ne oprejo na tako razlago teh direktiv, ki bi bila v nasprotju z navedenimi temeljnimi pravicami ali z drugimi splošnimi načeli prava Unije, kot je načelo sorazmernosti (točki 55 in 56).

V zvezi s tem je ugotovilo, da je zadevna nacionalna zakonodaja med drugim določala, da se odredba o razkritju zadevnih podatkov lahko izda, če obstajajo dejanski indici o posegu v pravico intelektualne lastnine na delu, če zahtevane informacije lahko olajšajo preiskavo glede kršitve avtorske pravice ali posega vanjo in če so razlogi, ki upravičujejo to odredbo, pomembnejši od nevšečnosti ali škode, ki bi jo naslovnik odredbe lahko utrpel, ali od vseh nasprotnih interesov v zvezi odredbo (točka 58).

Zato je Sodišče odločilo, da direktivi 2002/58/ES in 2004/48/ES ne nasprotujeta nacionalni zakonodaji, kot je bila ta v postopku v glavni stvari, ker je ta zakonodaja omogočala nacionalnemu sodišču, pri katerem je oseba s procesnim upravičenjem vložila prošnjo za odredbo o razkritju osebnih podatkov, da glede na okoliščine vsakega primera in ob ustreznem upoštevanju zahtev, ki izhajajo iz načela sorazmernosti, pretehta obstoječe nasprotne interese (točka 61 in izrek).

V. Nacionalni nadzorni organi

1. Obseg zahteve po neodvisnosti

Sodba z dne 9. marca 2010 (veliki senat), Komisija/Nemčija (C-518/07, EU:C:2010:125)²⁸

Komisija je s tožbo Sodišču predlagala, naj ugotovi, da Zvezna republika Nemčija s tem, da je nadzorne organe, odgovorne za spremljanje obdelave osebnih podatkov v zasebnem sektorju v različnih deželah, podvrgla državnemu nadzoru in tako nepravilno prenesla zahtevo po „popolni neodvisnosti“ organov, odgovornih za zagotavljanje varstva teh podatkov, ni izpolnila obveznosti iz člena 28(1), drugi pododstavek, Direktive 95/46/ES.

Zvezna republika Nemčija je trdila, da člen 28(1), drugi pododstavek, Direktive 95/46/ES zahteva funkcionalno neodvisnost nadzornih organov v tem smislu, da morajo biti ti organi neodvisni od zasebnega sektorja, ki je podvržen njihovemu nadzoru, in da ne smejo biti izpostavljeni zunanjim vplivom. Menila je, da državni nadzor, ki se izvaja v nemških deželah, ni tak zunanji vpliv, temveč le nadzorni mehanizem znotraj uprave, ki ga izvajajo organi, ki pripadajo istemu upravnemu aparatu kot nadzorni organi in morajo kot ti izpolnjevati cilje Direktive 95/46/ES.

Sodišče je razsodilo, da je namen jamstva neodvisnosti nacionalnih nadzornih organov, določenega z Direktivo 95/46/ES, zagotoviti učinkovit in zanesljiv nadzor nad spoštovanjem določb na področju varstva posameznikov pri obdelavi osebnih podatkov, zato ga je treba tudi razlagati glede na ta cilj. Ta cilj ni bil določen zaradi dodelitve posebnega statusa tem organom in njihovim zastopnikom, temveč za krepitev varstva oseb in organov, na katere se odločbe teh organov nanašajo, zaradi česar morajo nadzorni organi pri izvajanju nalog ravnati objektivno in nepristransko (točka 25).

Sodišče je ugotovilo, da morajo biti ti nadzorni organi, odgovorni za spremljanje obdelave osebnih podatkov v zasebnem sektorju, neodvisni, tako da lahko svoje naloge izvajajo brez zunanjega vpliva. Ta neodvisnost ne izključuje le vsakršnega vpliva nadziranih organov, temveč tudi kakršno koli navodilo in drug zunanji vpliv, bodisi neposreden bodisi posreden, ki bi lahko ogrožal navedene organe pri izvajanju njihove naloge ohranjanja pravega ravnotežja med varstvom pravice do zasebnosti in prostim pretokom osebnih podatkov. Že samo tveganje, da lahko državni organi izvajajo politični vpliv na odločitve nadzornih organov, zadostuje, da je ovirano neodvisno izvajanje nalog teh organov. Po eni strani bi lahko šlo za „vnaprejšnjo poslušnost“ teh organov z vidika prakse odločanja državnega organa. Po drugi strani pa vloga varuhov pravice do zasebnosti, ki naj bi jo imeli navedeni organi, zahteva, da so njihove odločitve in s tem organi brez kakršnega koli suma pristranskosti. Po mnenju Sodišča zato državni nadzor nad nadzornimi organi ni združljiv z zahtevo po neodvisnosti (točke 30, 36, 37 in izrek).

Sodba z dne 16. oktobra 2012 (veliki senat), Komisija/Avstrija (C-614/10, EU:C:2012:631)

Komisija je s tožbo Sodišču predlagala, naj ugotovi, da Avstrija s tem, da ni sprejela vseh potrebnih določb, zato da bi v Avstriji veljavna zakonodaja izpolnjevala merilo neodvisnosti v zvezi z Datenschutzkommission (komisija za varstvo podatkov), ki je bila ustanovljena kot nadzorni organ za varstvo osebnih podatkov, ni izpolnila obveznosti iz člena 28(1), drugi pododstavek, Direktive 95/46/ES.

Sodišče je ugotovilo, da Avstrija ni izpolnila obveznosti ter da merila neodvisnosti nadzornega organa iz Direktive 95/46/ES posledično ne izpolnjuje država članica, ki sprejme ureditev, na katere podlagi je član

²⁸ Ta sodba je bila predstavljena v Letnem poročilu 2010, str. 31.

administrator navedenega organa državni uradnik pod službenim nadzorom, čigar urad je vključen v službe nacionalne vlade, in v zvezi s katerim ima predsednik vlade brezpogojno pravico do obveščenosti o vseh vidikih vodenja navedenega organa (točka 66 in izrek).

Sodišče je najprej spomnilo, da izraz „popolnoma neodvisno“ iz člena 28(1), drugi pododstavek, Direktive 95/46/ES pomeni, da morajo biti nadzorni organi neodvisni, tako da lahko izvajajo svoje naloge brez zunanje vpliva. V zvezi s tem okoliščina, da ima tak organ funkcionalno neodvisnost, ker so njegovi člani pri opravljanju funkcije neodvisni in niso vezani na nobena navodila, sama po sebi ne zadošča, da bi bil navedeni nadzorni organ obvarovan pred vsakršnim zunanjim vplivom. Namen neodvisnosti, ki se zahteva v tem okviru, ni namreč izključiti le neposredni vpliv v obliki navodil, ampak tudi vsakršno obliko posrednega vpliva, ki lahko usmerja odločitve nadzornega organa. Poleg tega morajo biti glede na vlogo varuhov pravice do zasebnosti, ki jo imajo navedeni organi, njihove odločitve in s tem organi brez kakršnega koli suma pristranskosti (točke od 41 do 43 in 52).

Sodišče je pojasnilo, da za izpolnitev pogoja neodvisnosti iz zgoraj navedene določbe Direktive 95/46/ES ni potrebno, da ima nadzorni organ svojo proračunsko rubriko, kakor določa člen 43(3) Uredbe (ES) št. 45/2001. Države članice namreč niso zavezane, da v nacionalno zakonodajo vključijo določbe, ki so podobne tistim iz poglavja V Uredbe (ES) št. 45/2001, da bi svojemu nadzornemu organu ali nadzornim organom zagotovile popolno neodvisnost, in lahko tako z vidika proračunskega prava določijo, da spada nadzorni organ v neki oddelek ministrstva. Vendar zagotovitev osebja in potrebne opreme takemu organu temu ne sme preprečevati, da bi bil pri opravljanju nalog „popolnoma neodvisen“ v smislu člena 28(1), drugi pododstavek, Direktive 95/46/ES (točka 58).

Sodba z dne 8. aprila 2014 (veliki senat), Komisija/Madžarska (C-288/12, EU:C:2014:237)²⁹

V tej zadevi je Komisija Sodišču predlagala, naj ugotovi, da Madžarska s tem, da je predčasno prekinila mandat nadzornega organa za varstvo osebnih podatkov, ni izpolnila obveznosti na podlagi Direktive 95/46/ES.

Sodišče je razsodilo, da obveznosti na podlagi Direktive 95/46/ES ne izpolni država članica, ki predčasno prekine mandat nadzornega organa za varstvo osebnih podatkov (točka 62 in točka 1 izreka).

V skladu z navedbami Sodišča namreč neodvisnost, ki jo morajo imeti nadzorni organi, pristojni za spremljanje obdelave navedenih podatkov, izključuje zlasti vsakršno navodilo in kateri koli drug zunanji vpliv, bodisi neposreden bodisi posreden, ki bi lahko usmerjal odločitve teh nadzornih organov in tako ogrožal njihovo opravljanje naloge ohranjanja pravega ravnotežja med pravnim varstvom zasebnosti in prostim pretokom osebnih podatkov (točka 51).

Poleg tega je Sodišče spomnilo, da funkcionalna neodvisnost sama po sebi ne zadošča, da bi bili nadzorni organi obvarovani pred vsakršnim zunanjim vplivom, saj že samo tveganje, da lahko državni nadzorni organi izvajajo politični vpliv na odločitve nadzornih organov, zadostuje, da je ovirano neodvisno izvajanje nalog teh organov. Če pa bi lahko vsaka država članica prekinila mandat nadzornega organa pred njegovim prvotno določenim iztekom, ne da bi pri tem spoštovala pravila in jamstva, ki so bila za to predhodno določena z zakonodajo, ki se uporablja, bi lahko nevarnost take predčasne prekinitve, ki bi temu organu grozila med izvrševanjem njenega mandata, povzročila njegovo poslušnost do oblasti, ki ne bi bila v skladu z navedeno zahtevo po neodvisnosti. Poleg tega v takem položaju ne bi bilo mogoče šteti, da lahko nadzorni organ v katerih koli okoliščinah deluje brez kakršnega koli suma pristranskosti (točke od 52 do 55).

29 Ta sodba je bila predstavljena v Letnem poročilu 2014, str. 57.

2. Določitev prava, ki se uporabi, in pristojnega nadzornega organa

*Sodba z dne 1. oktobra 2015, Weltimmo (C-230/14, EU:C:2015:639)*³⁰

Nemzeti Adatvédelmi és Információszabadság Hatóság (nacionalni organ za varstvo podatkov in svobodo obveščanja, Madžarska) je družbi Weltimmo, ki je bila registrirana na Slovaškem in ki upravlja spletna mesta z nepremičninskimi oglasi za nepremičnine na Madžarskem, naložil globo, ker ta družba s teh mest ni izbrisala osebnih podatkov oglaševalcev, čeprav so ti to zahtevali, in je te podatke posredovala agencijam za izterjavo dolgov, da bi dosegla plačilo neplačanih računov. Po mnenju madžarskega nadzornega organa je družba Weltimmo s tem kršila madžarski zakon, s katerim je bila prenesena Direktiva 95/46/ES.

Kúria (vrhovno sodišče, Madžarska), ki mu je bila predložena kasacijska pritožba, je dvomilo o določitvi prava, ki se uporabi, in o pooblastilih, ki jih ima madžarski nadzorni organ glede na člena 4(1) in 28 Direktive 95/46/ES. Zato je Sodišče v predhodno odločanje predložilo več vprašanj.

Sodišče je v zvezi z nacionalnim pravom, ki se uporabi, razsodilo, da člen 4(1)(a) Direktive 95/46/ES dopušča uporabo zakonodaje o varstvu osebnih podatkov države članice, ki ni tista, v kateri je upravljavec teh podatkov registriran, če ta upravljavec prek poslovne enote na ozemlju te države članice opravlja dejansko in resnično, čeprav majhno, dejavnost, v katere okviru se izvaja ta obdelava. Da bi predložitveno sodišče ugotovilo, ali to drži, lahko zlasti upošteva, prvič, da je dejavnost upravljavca, v katere okviru ta obdelava poteka, upravljanje spletnih strani z nepremičninskimi oglasi za nepremičnine na ozemlju te države članice, ki so sestavljeni v jeziku te države, in da je zato ta dejavnost večinoma ali v celoti usmerjena v navedeno državo članico. Drugič, predložitveno sodišče lahko upošteva, da ima ta upravljavec zastopnika v navedeni državi članici, ki je zadolžen za izterjavo terjatev, ki izhajajo iz te dejavnosti, in za zastopanje upravljavca v upravnih in sodnih postopkih v zvezi z obdelavo zadevnih podatkov. Sodišče pa je pojasnilo, da ni upoštevno vprašanje državljanstva oseb, ki jih zadeva ta obdelava podatkov (točka 41 in točka 1 izreka).

Glede pristojnosti in pooblastil nadzornega organa, ki odloča o pritožbah v skladu s členom 28(4) Direktive 95/46/ES, je Sodišče ugotovilo, da lahko ta organ te pritožbe obravnava ne glede na pravo, ki se uporablja, in celo preden izve, katero nacionalno pravo se uporablja za obravnavano obdelavo (točka 54). Vendar če ugotovi, da se uporabi pravo druge države članice, ne more naložiti sankcij zunaj ozemlja lastne države članice. V takem položaju mora na podlagi dolžnosti sodelovanja, ki jo določa člen 28(6) te direktive, nadzornemu organu te druge države članice predlagati, naj ugotovi morebitno kršitev tega prava in naloži sankcije, če jih to pravo dopušča, ter naj se po potrebi opre na informacije, ki mu jih je posredoval (točki 57 in 60 ter točka 2 izreka).

3. Pooblastila pristojnih nacionalnih nadzornih organov

Sodba z dne 6. oktobra 2015 (veliki senat), Schrems (C-362/14, EU:C:2015:650)

Sodišče je v teh zadevi (glej tudi razdelek III, naslovljen „Prenos osebnih podatkov v tretje države“) med drugim razsodilo, da so nacionalni nadzorni organi pristojni za nadzor prenosov osebnih podatkov v tretje države.

³⁰ Ta sodba je bila predstavljena v Letnem poročilu 2015, str. 49.

Sodišče je v zvezi s tem najprej ugotovilo, da imajo nacionalni nadzorni organi širok razpon pooblastil in da ta pooblastila, netaksativno našeta v členu 28(3) Direktive 95/46/ES, pomenijo potrebna sredstva za opravljanje njihovih nalog. Tako imajo navedeni organi med drugim preiskovalna pooblastila, kakršna so pooblastila za zbiranje vseh informacij, ki so potrebne za izvajanje njihovih nadzornih nalog, učinkovita pooblastila za posredovanje, kot je začasna ali dokončna prepoved obdelave, in tudi pooblastilo za sodelovanje v sodnih postopkih (točka 43).

Glede pooblastila za nadzor prenosov osebnih podatkov v tretje države je Sodišče razsodilo, da sicer iz člena 28(1) in (6) Direktive 95/46/ES res izhaja, da se pooblastila nacionalnih nadzornih organov nanašajo na obdelavo osebnih podatkov, ki poteka na ozemlju države članice, ki ji pripadajo ti organi, tako da na podlagi tega člena 28 navedeni organi nimajo pooblastil v zvezi z obdelavo teh podatkov, ki poteka na ozemlju tretje države (točka 44).

Vendar postopek prenosa osebnih podatkov iz države članice v tretjo državo sam po sebi pomeni obdelavo osebnih podatkov, ki poteka na ozemlju države članice. Ker so nacionalni nadzorni organi v skladu s členom 8(3) Listine in členom 28 Direktive 95/46/ES odgovorni za nadzor nad spoštovanjem predpisov Unije v zvezi z varstvom posameznikov glede obdelave osebnih podatkov, je tako vsak od teh organov pristojen za preveritev, ali prenos osebnih podatkov iz države članice, ki ji pripada, v tretjo državo izpolnjuje zahteve, določene v tej direktivi (točki 45 in 47).

VI. Ozemeljska veljavnost evropske zakonodaje

Sodba z dne 13. maja 2014 (veliki senat), Google Spain in Google (C-131/12, EU:C:2014:317)

Sodišče je v tej sodbi (glej tudi razdelek II.3, naslovljen „Pojem ‚obdelava osebnih podatkov‘“, in razdelek IV.1., naslovljen „Pravica do ugovora zoper obdelavo osebnih podatkov („pravica biti pozabljen“)“) odločilo tudi o ozemeljskem področju uporabe Direktive 95/46/ES.

Sodišče je tako razsodilo, da se obdelava osebnih podatkov izvaja v okviru dejavnosti poslovne enote upravljavca na ozemlju države članice v smislu Direktive 95/46/ES, če upravljavec iskalnika, čeprav ima sedež v tretji državi, v eni od držav članic ustanovi podružnico ali hčerinsko družbo, ki se ukvarja s trženjem in prodajo oglasnega prostora na iskalniku, katerega dejavnost je usmerjena k prebivalcem tiste države članice (točki 55 in 60 ter točka 2 izreka).

V takih okoliščinah so namreč dejavnosti upravljavca iskalnika in dejavnosti njegove poslovne enote v državi članici, čeprav različne, neločljivo povezane, ker so dejavnosti, ki se nanašajo na oglasni prostor, sredstvo, s katerim iskalnik postane donosen, in ker je hkrati ta iskalnik sredstvo, ki omogoča izvajanje teh dejavnosti (točka 56).

VII. Pravica do dostopa javnosti do dokumentov institucij Evropske unije in varstvo osebnih podatkov

Sodba z dne 29. junija 2010 (veliki senat), Komisija/Bavarian Lager (C-28/08 P, EU:C:2010:378)

Bavarian Lager, družba, ki je bila ustanovljena za uvažanje nemškega piva za prodajo v točilnicah v Združenem kraljestvu, ni mogla prodajati svojega proizvoda, ker je bilo veliko število lastnikov točilnic v

Združenem kraljestvu vezanih s pogodbami o izključni nabavi, ki so jih zavezovale k oskrbovanju s pivom pri določenih pivovarnah.

V skladu z ureditvijo Združenega kraljestva o dobavi piva (v nadaljevanju: GBP) morajo britanske pivovarne poslovojem točilnic dopustiti možnost, da kupijo pivo druge pivovarne, če je to shranjeno v sodu. Vendar se večina piva, proizvedenega zunaj Združenega kraljestva, ni mogla šteti za „pivo, shranjeno v sodu“, v smislu GBP in zato ne spada na njeno področje uporabe. Ker je družba Bavarian Lager menila, da je navedena ureditev ukrep, ki ima enak učinek kot količinska omejitev uvoza, je pri Komisiji vložila pritožbo.

Med postopkom za ugotavljanje kršitev, ki ga je Komisija sprožila proti Združenemu kraljestvu, so se predstavniki upravnih organov Skupnosti in britanskih upravnih organov ter predstavniki zveze pivovarn na skupnem trgu (CBMC) sestali na sestanku, ki je potekal 11. oktobra 1996. Komisija je po tem, ko so jo britanski organi obvestili o spremembi zadevne ureditve, na katere podlagi bi se dovolila prodaja ustekleničenega piva kot piva drugega porekla po zgledu piva, shranjenega v sodu, družbo Bavarian Lager obvestila o ustavitvi postopka zaradi neizpolnitve obveznosti.

Družba Bavarian Lager je vložila prošnjo, da bi pridobila zapisnik sestanka iz oktobra 1996 z navedbo imen vseh udeležencev, Komisija pa je z odločbo z dne 18. marca 2004 to prošnjo zavrnila in se pri tem sklicevala zlasti na varstvo zasebnosti teh oseb, ki se zagotavlja z uredbo o varstvu osebnih podatkov.

Družba Bavarian Lager je nato vložila tožbo pri Splošnem sodišču, s katero je predlagala razglasitev ničnosti te odločbe Komisije. Splošno sodišče je s sodbo z dne 8. novembra 2007 odločbo Komisije razglasilo za nično, ker je menilo, da le vključitev imen zadevnih oseb na seznam oseb, ki so sodelovale na sestanku v imenu subjekta, ki so ga zastopale, ne oslabi in ne ogroža zasebnosti teh oseb. Komisija je ob intervenciji Združenega kraljestva in Sveta zato proti tej sodbi Splošnega sodišča vložila pritožbo pri Sodišču.

Sodišče je najprej navedlo, da če je namen prošnje, ki temelji na Uredbi (ES) št. 1049/2001³¹ o dostopu do dokumentov pridobiti dostop do dokumentov, ki vsebujejo osebne podatke, postanejo določbe Uredbe (ES) št. 45/2001 v celoti uporabljive, vključno z določbo, na katere podlagi mora prejemnik osebnih podatkov dokazati potrebo po razkritju teh podatkov, in določbo, ki posamezniku, na katerega se nanašajo osebni podatki, podeljuje pravico, da na nujni zakoniti podlagi v zvezi s svojim posebnim položajem kadar koli ugovarja obdelavi podatkov, ki se nanašajo nanj (točka 63).

Nato je Sodišče ugotovilo, da seznam udeležencev sestanka, opravljenega v okviru postopka za ugotavljanje kršitev, ki je v zapisniku navedenega sestanka, vsebuje osebne podatke v smislu člena 2(a) Uredbe (ES) št. 45/2001, ker se lahko iz njega ugotovi istovetnost oseb, ki so sodelovale na tem sestanku (točka 70).

Nazadnje je ugotovilo, da je Komisija s tem, da je zahtevala, da se dokaže potreba po posredovanju teh osebnih podatkov petih oseb, ki niso dale izrecnega soglasja za posredovanje osebnih podatkov, ravnala v skladu z določbami člena 8(b) navedene uredbe (točka 77).

Če namreč v okviru prošnje za dostop do zapisnika sestanka na podlagi Uredbe (ES) št. 1049/2001 ni predložena nobena izrecna in zakonita utemeljitev niti noben prepričljiv argument, da bi se dokazala potreba po posredovanju teh osebnih podatkov, Komisija ne more pretehtati različnih interesov zadevnih strank. Prav tako ne more preveriti, ali ni nobenega razloga, iz katerega bi se morda s tem prenosom

31 Uredba Evropskega parlamenta in Sveta (ES) št. 1049/2001 z dne 30. maja 2001 o dostopu javnosti do dokumentov Evropskega parlamenta, Sveta in Komisije (UL, posebna izdaja v slovenščini, poglavje 1, zvezek 3, str. 331).

poseglo v zakonite interese posameznikov, na katere se nanašajo osebni podatki, kot določa člen 8(b) Uredbe št. 45/2001.³²

Sodba z dne 16. julija 2015, ClientEarth in PAN Europe/EFSA (C-615/13 P, EU:C:2015:489)

Evropska agencija za varnost hrane (EFSA) je ustanovila delovno skupino za pripravo smernic za navedbo načina izvajanja člena 8(5) Uredbe (ES) št. 1107/2009,³³ v skladu s katerim vlagatelj zahtevka za registracijo dajanja fitofarmaceutskih sredstev v promet dokumentaciji priloži strokovno pregledano javno dostopno znanstveno literaturo, ki jo določa EFSA, o aktivnih snoveh in njihovih relevantnih metabolitih v zvezi s stranskimi učinki na zdravje, okolje in neciljne vrste.

Osnutek smernic je bil predmet javnega posvetovanja, tako da sta ClientEarth in Pesticide Action Network Europe (PAN Europe) predložili pripombe na ta osnutek. V tem okviru sta EFSI skupaj poslali zahtevo za dostop do več dokumentov v zvezi s pripravo osnutka smernic, vključno s pripombami zunanjih strokovnjakov.

EFSA je združenjema ClientEarth in PAN Europe odobrila dostop do zlasti posamičnih pripomb zunanjih strokovnjakov glede osnutka smernic. Vendar je navedla, da je v skladu s členom 4(1)(b) Uredbe št. 1049/2001 in zakonodajo Unije v zvezi z varstvom osebnih podatkov, zlasti Uredbo (ES) št. 45/2001, skrila imena teh strokovnjakov. V zvezi s tem je navedla, da razkritje imen teh strokovnjakov ustreza prenosu osebnih podatkov v smislu člena 8 Uredbe (ES) št. 45/2001 in da pogoji za tak prenos, navedeni v tem členu, v obravnavanem primeru niso izpolnjeni.

ClientEarth in PAN Europe sta zato pri Splošnem sodišču vložili tožbo za razglasitev ničnosti navedene odločbe EFSE. Splošno sodišče je to tožbo zavrnilo, zato sta ClientEarth in PAN Europe pri Sodišču vložili pritožbo zoper sodbo³⁴ Splošnega sodišča.

Sodišče je na prvem mestu navedlo, da bi zahtevana informacija omogočila, da se določeni strokovnjak poveže z določeno pripombo, zato se ta informacija nanaša na določeno fizično osebo in torej pomeni skupek osebnih podatkov v smislu člena 2(a) Uredbe (ES) št. 45/2001. Ker pojma „osebni podatek“ v smislu člena 2(a) Uredbe (ES) št. 45/2001 in „podatki o zasebnem življenju“ nista zamenljiva, je Sodišče poleg tega ugotovilo, da je trditev ClientEarth in PAN Europe, da sporna informacija ne spada pod zasebno življenje zadevnih strokovnjakov, brezpredmetna (točki 29 in 32).

Sodišče je na drugem mestu preučilo trditev ClientEarth in PAN Europe, ki je temeljila na vzdušju nezaupanja v razmerju do EFSE, ki je pogosto obtožena pristranskosti, ker sodeluje s strokovnjaki, ki imajo osebne interese, ki jih narekujejo njihove vezi z industrijskim sektorjem, in na nujnosti zagotavljanja preglednosti postopka odločanja tega organa. Ta trditev je bila oprta na študijo, ki dokazuje vezi večine strokovnjakov, članov delovne skupine EFSE, z industrijskimi lobiji. V zvezi s tem je Sodišče razsodilo, da se je pridobitev spornih informacij izkazala za nujno, da se omogoči konkretna preveritev nepristranskosti vsakega od teh strokovnjakov pri opravljanju njegove znanstvene naloge v službi EFSE. Sodišče je zato sodbo Splošnega sodišča razveljavilo, ker je ugotovilo, da je Splošno sodišče napačno presodilo, da trditev ClientEarth in PAN Europe ni zadoščala za dokaz potrebe po prenosu sporne informacije (točke od 57 do 59).

Sodišče je na tretjem mestu za presojo zakonitosti sporne odločbe EFSE preučilo še, ali je obstajal razlog, na katerega podlagi bi bilo mogoče domnevati, da bi ta prenos lahko posegel v zakonite interese

³² Ta sodba je bila predstavljena v Letnem poročilu 2010, str. 14.

³³ Uredba (ES) št. 1107/2009 Evropskega parlamenta in Sveta z dne 21. oktobra 2009 o dajanju fitofarmaceutskih sredstev v promet in razveljavitvi direktiv Sveta 79/117/EGS in 91/414/EGS (UL L 309, 24.11.2009, str. 1).

³⁴ Sodba Splošnega sodišča z dne 13. septembra 2013, ClientEarth in PAN Europe/EFSA (T-214/11, EU:T:2013:483).

posameznikov, na katere se nanašajo osebni podatki. V zvezi s tem je ugotovilo, da je trditev EFSE, da bi razkritje spornih informacij pomenilo nevarnost posega v zasebno življenje ali integriteto navedenih strokovnjakov, splošen preudarek, ki v obravnavanem primeru ni podprt z nobenim drugim dokazom. Sodišče je menilo, nasprotno, da bi tako razkritje lahko odpravilo sume o zadevni pristranskosti ali bi zadevnim strokovnjakom ponudilo priložnost, da izpodbijajo – po potrebi s pravnimi sredstvi, ki so na voljo – utemeljenost teh trditev o pristranskosti. Sodišče je glede na te elemente odločbo EFSE razglasilo za nično (točki 69 in 73).

* * *

Sodbe, navedene v tem prikazu, so v Seznamu sodne prakse v rubrikah 1.04.03.07, 1.04.03.08, 1.04.03.11, 2.04, 2.05.00, 4.11.01 in 4.11.07.