SODIŠČE EVROPSKE UNIJE
DIREKTORAT ZA RAZISKAVE IN DOKUMENTACIJO

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. Osebni 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 in družinskega 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 bila v tem pogledu osrednji pravni akt Unije na tem

[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. novembra 2003, razveljavljena s 25. majem 2018 (glej opombo 5).

področju. Z njo so bili opredeljeni splošni pogoji, ki so urejali zakonitost obdelave teh podatkov in pravice zadevnih oseb, ter je bila med drugim določena ustanovitev neodvisnih nadzornih organov v državah članicah.

Nato je Direktivo 95/46 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] Omeniti je treba, da namerava zakonodajalec Unije pregledati to direktivo. V zvezi s tem je Komisija 10. januarja 2017 vložila predlog za nadomestitev te direktive z uredbo o zasebnosti in elektronskih komunikacijah[4].

Poleg tega je bilo v okviru območja svobode, varnosti in pravice (prejšnja člena 30 in 31 PEU) z Okvirnim sklepom 2008/977/PNZ[5] do maja 2018 urejeno varstvo osebnih podatkov na področju pravosodnega sodelovanja v kazenskih in policijskih zadevah.

Evropska unija je leta 2016 prenovila celovit pravni okvir na tem področju. Za to je sprejela Uredbo (EU) 2016/679[6] o varstvu osebnih podatkov (v nadaljevanju: Splošna uredba o varstvu podatkov), s katero je bila razveljavljena Direktiva 95/46 in ki se uporablja od 25. maja 2018, ter Direktivo (EU) 2016/680[7] o varstvu navedenih podatkov v kazenskih zadevah, s katero je bil razveljavljen Okvirni sklep 2008/977/PNZ in za katero je bil rok za prenos za države članice določen na 6. maj 2018.

Nazadnje, v okviru obdelave osebnih podatkov v institucijah in organih EU je bilo varstvo osebnih podatkov najprej zagotovljeno z Uredbo (ES) št. 45/2001[8]. S to uredbo je bila zlasti omogočena ustanovitev Evropskega nadzornika za varstvo podatkov leta 2004. Leta 2018 je Evropska unija dobila nov pravni okvir na tem področju, zlasti s sprejetjem Uredbe (EU) 2018/1725[9], s katero sta bila razveljavljena Uredba št. 45/2001 in Sklep št. 1247/2002/ES[10] ter ki se uporablja od 11. decembra 2018. Za zagotovitev usklajenega pristopa k varstvu osebnih podatkov po vsej Uniji se s to novo uredbo pravila na tem področju čim bolj usklajujejo z ureditvijo, ki je bila uvedena s Splošno uredbo o varstvu podatkov.

---

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. decembra 2009.

3 Direktiva 2002/58 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 2006, L 105, 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 pravici 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 Predlog Uredbe Evropskega parlamenta in Sveta o spoštovanju zasebnega življenja in varstvu osebnih podatkov na področju elektronskih komunikacij ter razveljavitvi Direktive 2002/58/ES (uredba o e-zasebnosti), COM/2017/010 final - 2017/03 (COD).

5 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 2008, L 350, str. 60), razveljavljen od 6. maja 2018 (glej opombo 6).

6 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/ES (UL 2016, L 119, str. 1).

7 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 2016, L 119, str. 89).

8 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).

9 Uredba (EU) 2018/1725 Evropskega parlamenta in Sveta z dne 23. oktobra 2018 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.

10 Sklep št. 1247/2002/ES Evropskega parlamenta, Sveta in Komisije z dne 1. julija 2002 o predpisih in splošnih pogojih za izvajanje funkcije evropskega nadzornika za varstvo podatkov (UL, posebna izdaja v slovenščini, poglavje 1, zvezek 4, str. 43).

KAZALO

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)[11]

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. 1290/2005[12] in 259/2008[13], 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 št. 1290/2005 in Uredbe 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,

---

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

12 Uredba Sveta (ES) št. 1290/2005 z dne 21. junija 2005 o financiranju skupne kmetijske politike (UL 2005, L 209, 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 2013, L 347, str. 549).

13 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 2008, L 76, 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 2014, L 255, str. 59).

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 št. 1290/2005 in Uredbe 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 prejemali sredstva, pogostost ali vrsta in višina sredstev (točka 92 in točka 1 izreka). Vendar je Sodišče odločilo, da ni mogoče izpodbijati učinkov objave 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,[14] s katero je bila uvedena obveznost odvzema prstnih odtisov prosilcem za izdajo potnih listov, in med drugim trdil, da se s to uredbo krši ta 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 prosilce za izdajo potnih listov zavezuje, da dajo 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 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).

[14] 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 2004, L 385, str. 1), kakor je bila spremenjena z Uredbo (ES) št. 444/2009 Evropskega parlamenta in Sveta z dne 6. maja 2009 (UL 2009, L 142, str. 1).

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 št. 2252/2004 ne zajema obdelav odvzetih prstnih odtisov, ki bi presegale 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 nepooblaščene 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).

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)[15]

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) vloženih več pravnih sredstev na ustavni ravni, s katerimi je bila predlagana razglasitev ničnosti nacionalnega predpisa, s katerim je bila Direktiva 2006/24 prenesena v avstrijsko pravo.

Irsko in avstrijsko sodišče sta s svojima predlogoma za sprejetje predhodne odločbe Sodišče vprašali o veljavnosti Direktive 2006/24 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 zaradi nalaganja takih obveznosti ponudnikom posebej resno poseganje v temeljni pravici do 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

[15] Ta sodba je bila predstavljena v Letnem poročilu 2014, str. 55.

temeljnih pravic do 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 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, 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 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. Spoštovanje pravice 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)[16]

Sodišču sta bili po sodbi Digital Rights Ireland in Seitlinger in drugi, s katero je bila ugotovljena neveljavnost Direktive 2006/24 (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.

[16] Ta sodba je bila predstavljena v Letnem poročilu 2016, str. 55.

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 hranjenja podatkov, na podlagi katerega 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, 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 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 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 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 ureditev 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 splošne ureditve s tega področja

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

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 ameriškimi organi. Komisija je ob koncu teh pogajanj 14. maja 2004 sprejela Odločbo 2004/535/ES,[17] 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/ES[18] 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.

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. 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

[17] 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 2004, L 235, str. 11).

[18] 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 2004, L 183, str. 83).

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 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 ničen (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 tega 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, 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 alinea, 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 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, 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 izjemo, določeno v členu 3(2), druga alinea, te direktive, razlagati restriktivno (točke od 27 do 29). 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)[19]

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 odvračanja 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, 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 (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, 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).

[19] 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 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, 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 (točke 31 in od 36 do 40).

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 (točki 42 in 43).

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, 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 ne zajemata izpitnih vprašanj, ki kot taka niso osebni podatki kandidata (točki 56 in 58).

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 (točka 62 in izrek).

3. Pojem „obdelava osebnih podatkov“

Sodba z dne 6. novembra 2003 (veliki senat), 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.

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 državljan je 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.

Sodišče je tako 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).

Sodba z dne 10. julija 2018 (veliki senat), Jehovan todistajat (C-25/17, ECLI:EU:C:2018:551)[20]

Finski organ za varstvo podatkov je sprejel odločbo, s katero je skupnosti Jehovovih prič prepovedal zbiranje ali obdelavo osebnih podatkov v okviru oznanjevanja od vrat do vrat, ki ga njeni člani opravljajo, ne da bi spoštovali pogoje finske zakonodaje o obdelavi teh podatkov. Člani te skupnosti namreč v okviru oznanjevanja od vrat do vrat delajo zapiske o obiskih oseb, ki jih ti člani ali navedena skupnost ne poznajo. Ti podatki so zbrani v beležkah, da bi jih bilo mogoče najti za potrebe morebitnega poznejšega obiska, ne da bi zadevne osebe za to dale soglasje ali bile o tem obveščene. Glede tega je dala skupnost Jehovovih prič svojim članom navodila glede beleženja teh podatkov, ki so vsebovana vsaj v eni od revij o oznanjevanju.

Sodišče je razsodilo, da zbiranje osebnih podatkov, ki ga opravijo člani verske skupnosti med oznanjevanjem od vrat do vrat, in poznejša obdelava teh podatkov ne spadata k izjemam od področja uporabe Direktive 95/46, ker ne gre ne za obdelavo osebnih podatkov med dejavnostjo iz člena 3(2), prva alinea, te direktive ne za obdelavo osebnih podatkov, ki jo opravljajo fizične osebe med popolnoma osebnimi ali domačimi dejavnostmi, v smislu člena 3(2), druga alinea, navedene direktive (točka 51 in točka 1 izreka).

[20] Ta sodba je bila objavljena v Letnem poročilu 2018, str. 80 in 81.

Sodba z dne 14. februarja 2019, Buivids (C-345/17, EU:C:2019:122)

Sodišče je v tej sodbi na eni strani obravnavalo razlago področja uporabe Direktive 95/46, na drugi strani pa razlago pojma „obdelava osebnih podatkov zgolj v novinarske namene“ iz člena 9 te direktive.

Ta sodba je bila izdana v okviru predloga za sprejetje predhodne odločbe, ki ga je vložilo vrhovno sodišče Latvije, pred katerim je potekal spor med S. Buividsom (v nadaljevanju: pritožnik) in nacionalnim organom za varstvo podatkov v zvezi s tožbo za razglasitev ničnosti odločbe tega organa, s katero je bilo ugotovljeno, da je ta oseba kršila nacionalno zakonodajo s področja varstva osebnih podatkov, ker je na spletnem mestu objavila videoposnetek, ki ga je posnela sama, o tem, kako v prostorih nacionalne policijske postaje med postopkom zaradi upravnega prekrška podaja izjavo. Tako je pritožnik po tem, ko sta nižjestopenjski sodišči njegovo tožbo zavrnili, pri vrhovnem sodišču vložil kasacijsko pritožbo. Pred navedenim sodiščem se je skliceval na pravico do svobode izražanja, pri čemer je trdil, da da so bili na zadevnem videoposnetku prikazani uradniki nacionalne policije, torej javne osebe, na javno dostopnem mestu in da se zato za te osebe ne uporabljajo določbe zakona o varstvu podatkov.

Sodišče je na prvem mestu v zvezi s področjem uporabe Direktive 95/46 navedlo, da, prvič, posnetki policistov, ki jih vsebuje zadevni videoposnetek, pomenijo osebne podatke, in da, drugič, videoposnetek teh oseb, shranjen v pomnilniku kamere, ki jo je uporabil pritožnik, pomeni obdelavo osebnih podatkov. Sodišče je tako dodalo, da dejstvo, da se na spletnem mestu z videoposnetki, ki jih uporabniki lahko gledajo in delijo, objavi videoposnetek, na katerem se pojavijo osebni podatki, pomeni obdelavo teh podatkov v celoti ali delno z avtomatskimi sredstvi. Sodišče je poleg tega poudarilo, da navedeni posnetek in njegova objava ne spadata med določeni izjemi od področja uporabe Direktive 95/46, ki se nanašata zlasti na obdelavo osebnih podatkov v okviru dejavnosti, ki ne spadajo na področje uporabe te direktive, in na obdelavo med potekom popolnoma osebne ali domače dejavnosti. Zato je Sodišče ugotovilo, da videoposnetek policistov na policijski postaji med podajanjem izjave in objava tako shranjenega videoposnetka na spletnem mestu z videoposnetki, na katerem lahko uporabniki pošiljajo, gledajo in delijo te videoposnetke, spadata na področje uporabe te direktive (točke 31, 32, 35, 39, 42 in 43 ter točka 1 izreka).

Na drugem mestu je Sodišče v zvezi z obsegom pojma „obdelava osebnih podatkov zgolj v novinarske namene“ najprej opozorilo, da se na podlagi široke razlage pojma „novinarstvo“ izjeme in odstopanja iz člena 9 Direktive 95/46 uporabljajo za vsako osebo, ki se ukvarja z novinarstvom. Sodišče je tako razsodilo, da dejstvo, da pritožnik ni poklicni novinar, ne izključuje, da je mogoče snemanje zadevnega videoposnetka in njegovo prenašanje opredeliti za „obdelavo osebnih podatkov zgolj v novinarske namene“. Sodišče je poleg tega poudarilo, da je treba izjeme in odstopanja iz člena 9 Direktive 95/46 uporabiti le, če so potrebna za uskladitev dveh temeljnih pravic, in sicer pravice do zasebnosti in pravice do svobode izražanja. Sodišče je glede tega pojasnilo, da ni mogoče izključiti, da snemanje in objava zadevnega videoposnetka, ki sta bila opravljena, ne da bi bili policisti na tem videoposnetku obveščeni o tem snemanju in o tem, kakšen je je njegov namen, pomenita poseg v temeljno pravico teh oseb do zasebnosti. Zato je ugotovilo, da snemanje in objava zadevnega videoposnetka na spletnem mestu z videoposnetki lahko pomenita obdelavo osebnih podatkov zgolj v novinarske namene, če iz navedenega videoposnetka izhaja, da je edini namen navedenega snemanja in navedene objave razkritje

javnosti informacij, mnenj ali idej, kar pa mora preveriti predložitveno sodišče (točke 51, 52, 55, 63 in 67 ter točka 2 izreka).

Sodba z dne 22. junija 2021 (veliki senat), Latvijas Republikas Saeima (Kazenske točke) (C-439/19, EU:C:2021:504)

B je fizična oseba, ki so ji bile zaradi enega ali več cestnoprometnih prekrškov izrečene kazenske točke. Ceļu satiksmes drošības direkcija (direktorat za varnost v cestnem prometu, Latvija) (v nadaljevanju: CSDD) je te kazenske točke vpisal v nacionalni register vozil in njihovih voznikov.

Na podlagi latvijske ureditve o cestnem prometu[21] so informacije o kazenskih točkah, izrečenih voznikom vozil, vpisanih v ta register, dostopne javnosti ter jih CSDD posreduje vsaki osebi, ki to zahteva, ne da bi morala ta izkazati poseben interes za pridobitev teh informacij, in tudi gospodarskim subjektom za ponovno uporabo. Ker se je oseba B spraševala o zakonitosti te ureditve, je pri Latvijas Republikas Satversmes tiesa (ustavno sodišče, Latvija) vložila ustavno pritožbo, da bi to preučilo skladnost te ureditve s pravico do spoštovanja zasebnega življenja.

Ustavno sodišče je menilo, da mora pri presoji tega ustavnega prava upoštevati Splošno uredbo o varstvu podatkov. Tako je Sodišču predlagalo, naj pojasni obseg več določb Splošne uredbe o varstvu podatkov, da bi se ugotovila združljivost latvijske ureditve o cestnem prometu s to uredbo.

Sodišče je v sodbi, ki jo je izrekel veliki senat, razsodilo, da obdelava osebnih podatkov v zvezi s kazenskimi točkami pomeni „obdelavo osebnih podatkov v zvezi s kazenskimi obsodbami in prekrški [kaznivimi dejanji]“[22], za katero Splošna uredba o varstvu podatkov določa povečano varstvo zaradi posebne občutljivosti zadevnih podatkov (točke 10, 46, 74 in 94 ter točka 1 izreka).

V tem okviru je najprej ugotovilo, da so informacije v zvezi kazenskimi točkami osebni podatki in da to, da jih CSDD posreduje tretjim osebam, pomeni obdelavo, ki spada na stvarno področje uporabe Splošne uredbe o varstvu podatkov. To področje uporabe je namreč zelo široko in ta obdelava ne spada med izjeme od uporabe te uredbe (točke 60, 61 in 72).

Tako na eni strani za to obdelavo ne velja izjema, na podlagi katere se Splošna uredba o varstvu podatkov ne uporablja za obdelavo, opravljeno v okviru dejavnosti, ki ne spada na področje uporabe prava Unije.[23] Za to izjemo je treba šteti, da je njen edini namen izključiti s področja uporabe te uredbe obdelave osebnih podatkov, ki jih izvajajo državni organi v okviru dejavnosti, katere namen je ohraniti nacionalno varnost, ali v okviru dejavnosti, ki jo je mogoče razvrstiti v isto kategorijo. Te dejavnosti zajemajo zlasti tiste, katerih cilj je zaščita bistvenih funkcij države in temeljnih interesov družbe. Dejavnosti v zvezi z varnostjo v cestnem prometu pa ne uresničujejo tega cilja in jih zato ni mogoče razvrstiti v kategorijo dejavnosti, katerih cilj je ohranitev nacionalne varnosti (točke 62 in od 66 do 68).

---

21 Člen 14[1](2) Ceļu satiksmes likums (zakon o cestnem prometu) z dne 1. oktobra 1997 (Latvijas Vēstnesis, 1997, št. 274/276).
22 Člen 10 Splošne uredbe o varstvu podatkov.
23 člen 2(2)(a) Splošne uredbe o varstvu podatkov.

Na drugi strani posredovanje osebnih podatkov v zvezi s kazenskimi točkami prav tako ni obdelava, zajeta z izjemo, na podlagi katere se Splošna uredba o varstvu podatkov ne uporablja za obdelavo osebnih podatkov, ki jo opravljajo organi, pristojni v kazenskih zadevah.[24] Sodišče je namreč ugotovilo, da CSDD pri izvajanju navedenega posredovanja ni mogoče šteti za tak „pristojni organ“[25] (točke od 69 do 71).

Da bi Sodišče ugotovilo, ali dostop do osebnih podatkov v zvezi s cestnoprometnimi prekrški, kot so kazenske točke, pomeni obdelavo osebnih podatkov v zvezi s „prekrški [kaznivimi dejanji]“,[26] ki uživajo povečano varstvo, je ob opiranju med drugim na zgodovino nastanka splošne uredbe o varstvu podatkov ugotovilo, da ta pojem napotuje izključno na kazenskopravne kršitve. Vendar dejstvo, da so cestnoprometni prekrški v latvijskem pravnem sistemu opredeljeni kot prekrški, ni odločilno za presojo, ali ti prekrški spadajo pod pojem „prekršek [kaznivo dejanje]“, ker gre za avtonomen pojem prava Unije, ki ga je treba v vsej Uniji razlagati avtonomno in enotno. Tako je Sodišče, potem ko je opozorilo na tri upoštevna merila za presojo kazenskopravne narave kršitve, in sicer na pravno opredelitev kršitve v nacionalnem pravu, naravo kršitve in stopnjo strogosti izrečene sankcije, razsodilo, da zadevni cestnoprometni prekrški spadajo pod pojem „prekršek [kaznivo dejanje]“ v smislu Splošne uredbe o varstvu podatkov. Sodišče je v zvezi s prvima dvema meriloma ugotovilo, da čeprav kršitve v nacionalnem pravu niso opredeljene kot „kazenske“, lahko taka narava izhaja iz narave kršitve in zlasti iz represivnega cilja sankcije, ki se lahko zanjo izreče. V obravnavani zadevi pa ima dodelitev kazenskih točk za cestnoprometne prekrške, tako kot druge sankcije, ki jih je mogoče naložiti zaradi storitve teh prekrškov, med drugim tak represivni cilj. Sodišče je v zvezi s tretjim merilom ugotovilo, da le cestnoprometni prekrški, ki so dovolj resni, vključujejo dodelitev kazenskih točk in da se zato za take prekrške lahko izreče sankcija z določeno stopnjo strogosti. Poleg tega izrekanje takih točk običajno dopolnjuje naloženo sankcijo, vsota teh točk pa ima pravne posledice, ki lahko privedejo celo do izreka prepovedi vožnje (točke 77, 80, 85, od 87 do 90 in 93).

4. Pojem „zbirka osebnih podatkov“

Sodba z dne 10. julija 2018 (veliki senat), Jehovan todistajat (C-25/17, ECLI:EU:C:2018:551)

Sodišče je v tej sodbi (glej tudi razdelek II.3., naslovljen „Pojem ‚obdelava osebnih podatkov‘“) pojasnilo pojem „zbirka“ iz člena 2(c) Direktive 95/46.

Tako je Sodišče po tem, ko je opozorilo, da se ta direktiva uporablja za ročno obdelavo osebnih podatkov le, če podatki, ki se obdelujejo, sestavljajo del zbirke ali so namenjeni sestavljanju dela zbirke, razsodilo, da navedeni pojem zajema niz osebnih podatkov, zbranih med oznanjevanjem od vrat do vrat, v katerem so imena, naslovi in drugi podatki o obiskanih osebah, če so ti podatki strukturirani v skladu s posebnimi merili, ki v praksi omogočajo, da se ti podatki za potrebe poznejše uporabe enostavno najdejo. Da bi tak niz spadal pod ta pojem, ni potrebno, da je sestavljen iz kartotek, posebnih seznamov in drugih sistemov razvrščanja (točka 62 in točka 2

[24] Člen 2(2)(d) Splošne uredbe o varstvu podatkov.

[25] Člen 3, točka 7, Direktive (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 2016, L 119, str. 89).

[26] Člen 10 Splošne uredbe o varstvu podatkov.

izreka).

5. Pojem „upravljavec osebnih podatkov“

Sodba z dne 10. julija 2018 (veliki senat), Jehovan todistajat (C-25/17, ECLI:EU:C:2018:551)

Sodišče se je v tej zadevi (glej tudi razdelka II.3. in II.4., naslovljena „Pojem ‚obdelava osebnih podatkov‘“ oziroma „Pojem ‚zbirka osebnih podatkov‘“) izreklo o odgovornosti verske skupnosti za obdelavo osebnih podatkov v okviru oznanjevanja od vrat do vrat, ki ga organizira, usklajuje in spodbuja ta skupnost.

Sodišče je tako štelo, da obveznosti vsakogar, da ravna v skladu s pravili prava Unije o varstvu osebnih podatkov, ni mogoče šteti za poseg v organizacijsko avtonomijo verskih skupnosti. Glede tega je ugotovilo, da je treba člen 2(d) Direktive 95/46 v povezavi s členom 10(1) Listine razlagati tako, da omogoča, da se verska skupnost skupaj s svojimi oznanjevalci šteje za upravljavca osebnih podatkov, ki jih oznanjevalci obdelujejo med oznanjevanjem od vrat do vrat, ki ga ta skupnost organizira, usklajuje in spodbuja, pri čemer ni potrebno, da ima ta skupnost dostop do teh podatkov, niti ni treba dokazati, da je svojim članom dala pisne smernice ali navodila v zvezi s to obdelavo (točki 74 in 75 ter točka 3 izreka).

Sodba z dne 5. junija 2018 (veliki senat), Wirtschaftsakademie Schleswig Holstein (C-210/16, ECLI:EU:C:2018:388)[27]

Nemški organ za varstvo podatkov je kot nadzorni organ v smislu člena 28 Direktive 95/46 odredil nemški družbi, ki je specializirana na področju izobraževanja in ponuja svoje storitve usposabljanja prek strani oboževalcev na spletnem mestu družbenega omrežja Facebook, naj to stran izklopi. Navedeni organ je namreč ugotovil, da niti ta družba niti družba Facebook obiskovalcev strani oboževalcev nista obvestili o tem, da je drugonavedena družba s piškotki zbirala osebne podatke v zvezi z njimi, in da sta navedena družba in družba Facebook nato te podatke obdelovali.

Sodišče je v tem okviru pojasnilo pojem „upravljavec“ osebnih podatkov. Glede tega je štelo, da skrbnik strani oboževalcev, ki gostuje na Facebooku, kot je družba iz postopka v glavni stvari, z izbiro nastavitev (med drugim glede na svojo ciljno javnost in cilje upravljanja oziroma pospeševanja svojih dejavnosti) sodeluje pri določanju namena in sredstev obdelave osebnih podatkov obiskovalcev njegove strani oboževalcev. Zato je Sodišče ugotovilo, da je treba za tega skrbnika šteti, da je v Uniji solidarno z družbo Facebook Ireland (hčerinska družba ameriške družbe Facebook v Uniji) odgovoren za to obdelavo v smislu člena 2(d) Direktive 95/46 (točka 39).

[27] Ta sodba je bila predstavljena v Letnem poročilu 2018, str. 80.

Sodba z dne 29. julija 2019, Fashion ID (C-40/17, EU:C:2019:629)

Sodišče je v tej zadevi razvilo pojem „upravljavec“ z vidika vstavitve vtičnika („plug-in“) na spletno stran.

V obravnavani zadevi je nemško podjetje za prodajo modnih oblačil prek spleta Fashion ID na svoje spletno mesto vstavilo socialni vtičnik „všeč mi je“ družbenega omrežja Facebook. Zdi se, da se zaradi te vstavitve, kadar obiskovalec pregleduje spletno mesto podjetja Fashion ID, osebni podatki tega obiskovalca prenesejo na družbo Facebook Ireland. Ta prenos se izvede, ne da bi navedeni obiskovalec za to vedel ter ne glede na to, ali je član družbenega omrežja Facebook in ali je kliknil na Facebookov gumb „všeč mi je“.

Verbraucherzentrale NRW, nemško nepridobitno združenje za varstvo interesov potrošnikov, podjetju Fashion ID očita, da je družbi Facebook Ireland posredovalo osebne podatke obiskovalcev svojega spletnega mesta, prvič, brez njihove privolitve, in drugič, tako, da je kršilo obveznosti glede obveščanja, določene v predpisih o varstvu osebnih podatkov. Oberlandesgericht Düsseldorf (višje deželno sodišče v Düsseldorfu, Nemčija), ki mu je bil spor predložen, je Sodišče zaprosilo za razlago več določb Direktive 95/46.

Sodišče je najprej ugotovilo, da je upravljavca spletnega mesta, kot je podjetje Fashion ID, mogoče šteti za upravljavca v smislu člena 2(d) Direktive 95/46. Vendar je ta odgovornost omejena na postopek ali niz postopkov obdelave osebnih podatkov, za katere dejansko določa namene in sredstva, in sicer zbiranje in posredovanje s prenosom zadevnih podatkov. Sodišče pa je navedlo, da je na prvi pogled izključeno, da podjetje Fashion ID določa namene in sredstva naknadnih postopkov obdelave osebnih podatkov, ki jih izvaja družba Facebook Ireland po posredovanju podatkov zadnjenavedeni, tako da se za podjetje Fashion ID ne more šteti, da je upravljavec teh postopkov v smislu tega člena 2(d) (točki 76 in 85 ter točka 2 izreka).

Sodišče je poleg tega poudarilo, da je potrebno, da si upravljavec spletnega mesta in ponudnik socialnega vtičnika, kot je družba Facebook Ireland, s temi postopki obdelave prizadevata za zakoniti interes v smislu člena 7(f) Direktive 95/46, da bi bili ti postopki upravičeni glede vsakega od njiju (točka 97 in točka 3 izreka).

Nazadnje je Sodišče pojasnilo, da mora upravljavec spletnega mesta privolitev zadevne osebe, na katero se nanašata člen 2(h) in člen 7(a) Direktive 95/46, pridobiti samo v zvezi s postopki obdelave osebnih podatkov, za katere navedeni upravljavec spletnega mesta določi namene in sredstva. V takem primeru za navedenega upravljavca spletnega mesta prav tako velja obveznost zagotavljanja informacij, določena v členu 10 te direktive, pri tem pa mora zadnjenavedeni zadevno osebo obvestiti le o postopku ali nizu postopkov obdelave osebnih podatkov, za katere določi namene in sredstva (točka 106 in točka 4 izreka).

Sodba z dne 9. julija 2020, Land Hessen, C-272/19, EU:C:2020:535

Državljan, ki je pri odboru za peticije deželnega zbora zvezne dežele Hessen (Nemčija) vložil peticijo, je pri tem odboru vložil zahtevo za dostop do osebnih podatkov, ki se nanašajo nanj in jih je ta odbor shranil v okviru obravnave njegove peticije. V zvezi s svojo zahtevo se je skliceval na Splošno uredbo o varstvu podatkov, ki določa pravico posameznika, na katerega se nanašajo osebni podatki, da od upravljavca dobi dostop do osebnih podatkov, ki se nanašajo nanj.

Predsednik deželnega zbora zvezne dežele Hessen je to zahtevo zavrnil z obrazložitvijo, da je postopek obravnavanja peticije parlamentarna naloga in da se za deželni zbor Splošna uredba o varstvu podatkov ne uporablja.

Verwaltungsgericht Wiesbaden (upravno sodišče v Wiesbadnu, Nemčija), pri katerem je ta državljan začel postopek, je menilo, da nemško pravo ne podeljuje nobene pravice do dostopa do osebnih podatkov v okviru peticije, kakršna je bila ta v postopku v glavni stvari. Vendar bi po mnenju Verwaltungsgericht Wiesbaden (upravno sodišče v Wiesbadnu) taka pravica lahko izhajala iz Splošne uredbe o varstvu podatkov, zato je Sodišču postavilo vprašanje v zvezi s tem. Poleg tega je Verwaltungsgericht Wiesbaden (upravno sodišče v Wiesbadnu) podvomilo v lastno neodvisnost in torej v to, ali ima status sodišča, ki lahko Sodišču postavlja vprašanja za predhodno odločanje, zato je Sodišču postavilo tudi vprašanje v tem smislu.

Sodišče je v sodbi odgovorilo, da če odbor za peticije deželnega zbora zvezne dežele določene države članice sam ali skupaj z drugimi določa namene in sredstva obdelave osebnih podatkov, je treba ta odbor opredeliti kot „upravljavca“ v smislu Splošne uredbe o varstvu podatkov.[28] Obdelava osebnih podatkov, ki jo izvaja tak odbor, torej spada na področje uporabe te uredbe, zlasti določbe, s katero je posameznikom, na katere se nanašajo osebni podatki, podeljena pravica do dostopa do osebnih podatkov, ki se nanašajo nanje.[29]

Sodišče je med drugim ugotovilo, da dejavnosti odbora za peticije deželnega zbora zvezne dežele Hessen ne spadajo pod katero od izjem iz Splošne uredbe o varstvu podatkov. Priznalo je, da so te dejavnosti javne in značilne za to zvezno deželo, ker ta odbor posredno prispeva k parlamentarni dejavnosti, vendar je navedlo, da so te dejavnosti tudi politične in upravne narave. Poleg tega iz elementov, s katerimi je Sodišče razpolagalo, nikakor ni izhajalo, da te dejavnosti v obravnavanem primeru ustrezajo kateri od izjem iz Splošne uredbe o varstvu podatkov (točke od 71 do 74 in izrek).

6. Pogoji zakonitosti obdelave osebnih podatkov

Sodba z dne 16. decembra 2008 (veliki senat), Huber (C-524/06, EU:C:2008:724)[30]

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.

---

28 Člen 4, točka 7, Splošne uredbe o varstvu podatkov.
29 Člen 15 Splošne uredbe o varstvu podatkov.
30 Ta sodba je bila predstavljena v Letnem poročilu 2008, str. 41.

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 „nujnost“ obdelave v smislu člena 7(e) Direktive 95/46 najprej opozorilo, da gre za avtonomen pojem prava Unije, ki ga je treba razlagati tako, da popolnoma ustreza namenu Direktive 95/46, 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 shranjevanje in obdelava osebnih podatkov, ki so v okviru takega registra navedeni poimensko, nujni za statistične namene (točke 52, 66 in 68).

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 (vrhovno sodišče, 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.

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, s tem, da zahteva, da so navedeni podatki „iz javno dostopnih virov“, kot so našteti v členu 3(j) sistemskega 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, 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 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. Zato je Sodišče razsodilo, da člen 7(f) Direktive 95/46 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 47 in 48).

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 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 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, 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 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 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 njegovega 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 Slovenskej republiky (vrhovno sodišče Slovaške republike) 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 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 pooblaščeni 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 (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 javnosti oziroma 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 obstajali razlogi za omejitev nekaterih pravic iz členov 6 in 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).

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

Družba Orange România SA je ponudnica mobilnih telekomunikacijskih storitev na romunskem trgu. Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP) (nacionalni organ za nadzor nad obdelavo osebnih podatkov, Romunija) je z odločbo z dne 28. marca 2018 tej družbi naložil globo zaradi pridobivanja in hrambe kopij osebnih dokumentov svojih strank, ne da bi te v to izrecno privolile.

ANSPDCP je navedel, da je družba Orange România v obdobju od 1. do 26. marca 2018 sklepala pogodbe o zagotavljanju mobilnih telekomunikacijskih storitev, ki so vsebovale določilo, da so bile stranke obveščene o pridobitvi in hrambi kopije njihovega osebnega dokumenta za identifikacijo ter da so v to privolile. Okence v zvezi s tem določilom je označil upravljavec, preden je bila pogodba podpisana.

V teh okoliščinah je Tribunalul București (okrožno sodišče v Bukarešti, Romunija) Sodišče zaprosilo, naj pojasni, pod katerimi pogoji je mogoče privolitev strank v obdelavo osebnih podatkov šteti za veljavno.

Sodišče je najprej opozorilo, da pravo Unije[31] določa seznam primerov, v katerih je mogoče šteti, da je obdelava osebnih podatkov zakonita. Zlasti je potrebno, da je privolitev posameznika, na katerega se nanašajo osebni podatki, prostovoljna, posebna, informirana in nedvoumna.[32] Glede tega velja, da privolitev ni veljavna v primeru molka, vnaprej označenih okenc ali nedejavnosti (točke 34, 36, 37 in 39).

Poleg tega je, kadar je privolitev posameznika, na katerega se nanašajo osebni podatki, dana v pisni izjavi, ki se nanaša tudi na druge zadeve, potrebno, da se ta izjava predloži v razumljivi in lahko dostopni obliki ter v jasnem in preprostem jeziku. Za to, da se posamezniku, na katerega se nanašajo osebni podatki, zagotovi resnična svoboda izbire, pogodbene določbe le-tega ne smejo zavesti glede možnosti sklenitve pogodbe, tudi če zavrne privolitev v obdelavo svojih podatkov (točke 34, 36, 37, 39 in 41).

Sodišče je natančneje navedlo, da bi morala biti družba Orange România kot upravljavec obdelave osebnih podatkov zmožna dokazati zakonitost obdelave teh podatkov in v obravnavani zadevi torej obstoj veljavne privolitve svojih strank. V zvezi s tem glede na to, da ni kazalo, da bi zadevne stranke same označile okence v zvezi s pridobitvijo in hrambo kopij njihovih osebnih dokumentov, zgolj s tem, da je bilo to okence označeno, ni bilo mogoče dokazati pozitivnega izraza privolitve teh strank. Odločeno je bilo, da mora nacionalno sodišče v zvezi s tem opraviti potrebna preverjanja (točki 42 in 46).

V skladu z ugotovitvami Sodišča bi moralo nacionalno sodišče tudi presoditi, ali bi lahko zadevna pogodbena določila zadevne stranke zavedla glede možnosti sklenitve pogodbe ne glede na zavrnitev privolitve v obdelavo svojih podatkov, če ni pojasnila o tej možnosti. Poleg tega je Sodišče navedlo, da je družba Orange România v primeru, da stranka ni želela privoliti v obdelavo svojih podatkov, od nje zahtevala, naj pisno izjavi, da ne soglaša niti s pridobitvijo niti s hrambo kopije svojega osebnega dokumenta. Sodišče je ugotovilo, da lahko taka dodatna zahteva neupravičeno vpliva na svobodno izbiro, da se tej pridobitvi in tej hrambi nasprotuje. Vsekakor navedena družba glede na to, da je ona tista, ki mora dokazati, da so njene stranke z aktivnim ravnanjem izjavile privolitev v obdelavo svojih osebnih podatkov, ne more zahtevati od teh strank, da aktivno izjavijo svojo zavrnitev (točke od 49 do 51).

Sodišče je torej ugotovilo, da s pogodbo o zagotavljanju telekomunikacijskih storitev, ki vsebuje določilo, v skladu s katerim je bil posameznik, na katerega se nanašajo osebni podatki, obveščen

[31] Člen 7 Direktive 95/46 in člen 6 Splošne uredbe o varstvu podatkov.
[32] Člen 2(h) Direktive 95/46 in člen 4, točka 11, Splošne uredbe o varstvu podatkov.

o pridobitvi in hrambi kopije njegovega osebnega dokumenta za identifikacijo ter v skladu s katerim je v to privolil, ni mogoče dokazati, da je ta posameznik veljavno privolil v to pridobitev in hrambo, če je upravljavec obdelave podatkov pred podpisom te pogodbe označil okence, ki se nanaša na to določbo, če lahko pogodbena določila navedene pogodbe zavedejo posameznika, na katerega se nanašajo osebni podatki, glede možnosti sklenitve zadevne pogodbe, tudi če zavrne privolitev v obdelavo svojih podatkov, ali če ta upravljavec v prosto izbiro, da se takemu pridobivanju in hrambi nasprotuje, neupravičeno poseže s tem, da zahteva, da posameznik, na katerega se nanašajo osebni podatki, da bi zavrnil svojo privolitev, izpolni dodatni obrazec, ki to zavrnitev potrjuje (točka 52 in izrek).

Sodba z dne 12. maja 2021 (veliki senat), Bundesrepublik Deutschland (Interpolova rdeča mednarodna tiralica) (C-505/19, EU:C:2021:376)

Mednarodna organizacija kriminalistične policije (v nadaljevanju: Interpol) je leta 2012 na zahtevo Združenih držav in na podlagi naloga za prijetje, ki so ga izdali organi te države, razpisala rdečo mednarodno tiralico za WS, nemškim državljanom, da bi bil eventualno izročen navedeni državi. Kadar je oseba, na katero se taka mednarodna tiralica nanaša, izsledena v državi članici Interpola, mora ta država to osebo načeloma začasno prijeti oziroma nadzorovati ali omejiti njeno gibanje.

Vendar je bil že pred razpisom te rdeče mednarodne tiralice v Nemčiji zoper WS začet kazenski postopek, ki se je po mnenju predložitvenega sodišča nanašal na ista dejanja, kot so ta, na podlagi katerih je bila razpisana ta mednarodna tiralica. Ta postopek je bil pravnomočno ustavljen leta 2010, potem ko je WS plačal določen denarni znesek, in sicer v okviru posebnega postopka poravnave, določenega v nemškem kazenskem pravu. Bundeskriminalamt (zvezna uprava kriminalistične policije, Nemčija) je nato Interpol obvestila, da meni, da se zaradi tega prejšnjega postopka v obravnavani zadevi uporablja načelo *ne bis in idem*. To načelo, ki je določeno tako v členu 54 Konvencije o izvajanju Schengenskega sporazuma[33] kot tudi v členu 50 Listine, zlasti prepoveduje, da bi se zoper osebo, proti kateri je bil sodni postopek že pravnomočno končan, ponovno začel pregon za isto kaznivo dejanje.

Leta 2017 je WS pri Verwaltungsgericht Wiesbaden (upravno sodišče v Wiesbadnu, Nemčija) vložil tožbo proti Zvezni republiki Nemčiji, da bi se ji naložilo, naj sprejme ukrepe, potrebne za preklic te rdeče mednarodne tiralice. V tej tožbi se je WS poleg na kršitev načela *ne bis in idem* skliceval tudi na kršitev svoje pravice do prostega gibanja, zagotovljene s členom 21 PDEU, ker ni mogel iti v državo pogodbenico Schengenskega sporazuma ali v državo članico, ne da bi tvegal, da bo prijet. Menil je tudi, da je zaradi teh kršitev obdelava njegovih osebnih podatkov, navedenih v rdeči mednarodni tiralici, v nasprotju z Direktivo 2016/680, ki ureja varstvo osebnih podatkov na področju kazenskega prava.[34]

---

33 Konvencija o izvajanju Schengenskega sporazuma z dne 14. junija 1985 med vladami držav Gospodarske unije Beneluks, Zvezne republike Nemčije in Francoske republike o postopni odpravi kontrol na skupnih mejah (UL, posebna izdaja v slovenščini, poglavje 19, zvezek 2, str. 9; v nadaljevanju: Schengenska konvencija).

34 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 2016, L 119, str. 89).

V teh okoliščinah je upravno sodišče v Wiesbadnu odločilo, da Sodišču postavi vprašanja o uporabi načela *ne bis in idem* in, natančneje, o možnosti začasnega prijetja osebe, na katero se nanaša rdeča mednarodna tiralica, v položaju, kakršen je obravnavani. Poleg tega je želelo to sodišče, če se to načelo uporablja, izvedeti, kakšne so posledice te uporabe za obdelavo osebnih podatkov, navedenih v taki mednarodni tiralici, ki jo izvajajo države članice.

Sodišče je v sodbi, ki jo je izdalo v velikem senatu, med drugim razsodilo, da je treba določbe Direktive 2016/680 v povezavi s členom 54 Schengenske konvencije in členom 50 Listine razlagati tako, da ne nasprotujejo obdelavi osebnih podatkov, navedenih v rdeči mednarodni tiralici, ki jo je razpisal Interpol, dokler ni s pravnomočno sodno odločbo ugotovljeno, da se za dejanja, na katerih temelji ta mednarodna tiralica, uporablja načelo *ne bis in idem*, pri čemer je potrebno, da taka obdelava izpolnjuje pogoje, določene v tej direktivi (točka 121 in točka 2 izreka).

Glede vprašanja v zvezi z osebnimi podatki, navedenimi v Interpolovi rdeči mednarodni tiralici, je Sodišče navedlo, da vsako ravnanje v zvezi s temi podatki, kot je njihov vnos v seznam iskanih oseb države članice, pomeni „obdelavo“, ki spada na področje uporabe Direktive 2016/680.[35] Poleg tega je ugotovilo, prvič, da ima ta obdelava legitimen cilj, in drugič, da je ni mogoče šteti za nezakonito zgolj zato, ker bi se načelo *ne bis in idem* lahko uporabljalo za dejanja, na katerih temelji rdeča mednarodna tiralica.[36] Ta obdelava, ki jo opravljajo organi držav članic, se poleg tega lahko izkaže za nepogrešljivo ravno zato, da se preveri, ali se navedeno načelo uporablja (točke 111, 114, 116, 117 in 119).

V teh okoliščinah je Sodišče prav tako razsodilo, da Direktiva 2016/680 v povezavi s členom 54 Schengenske konvencije in členom 50 Listine ne nasprotuje obdelavi osebnih podatkov, navedenih v rdeči mednarodni tiralici, dokler ni v pravnomočni sodni odločbi ugotovljeno, da se v obravnavani zadevi uporablja načelo *ne bis in idem*. Vendar mora taka obdelava izpolnjevati pogoje, določene v tej direktivi. Tako mora biti med drugim potrebna za to, da pristojni nacionalni organ opravi naloge, ki jih izvaja zaradi preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj oziroma izvrševanja kazenskih sankcij[37] (točka 121 in točka 2 izreka).

Kadar pa se načelo *ne bis in idem* uporablja, ni več potrebno, da se osebni podatki, navedeni v Interpolovi rdeči mednarodni tiralici, vnesejo v sezname iskanih oseb držav članic, saj zoper zadevno osebo ni več mogoče začeti kazenskega pregona za dejanja, na katera se nanaša navedena mednarodna tiralica, in je zato za ista dejanja ni mogoče prijeti. Iz tega sledi, da mora imeti zadevna oseba možnost zahtevati izbris svojih podatkov. Če se ta vnos kljub temu ohrani, mu mora biti priloženo opozorilo, da se zadevne osebe zaradi načela *ne bis in idem* v državi članici ali državi pogodbenici ne sme več preganjati za ista dejanja (točka 120).

Sodba z dne 22. junija 2021 (veliki senat), Latvijas Republikas Saeima (Kazenske točke) (C-439/19, EU:C:2021:504)

35 Glej člen 2(1) in člen 3, točka 2, Direktive 2016/680.

36 Glej člen 4(1)(b) in člen 8(1) Direktive 2016/680.

37 Glej člen 1(1) in člen 8(1) Direktive 2016/680.

Sodišče je v tej sodbi (glej tudi razdelek II.3., naslovljen „Pojem ‚obdelava osebnih podatkov'") razsodilo, da Splošna uredba o varstvu podatkov nasprotuje ureditvi, ki Ceļu satiksmes drošības direkcija (direktorat za varnost v cestnem prometu, Latvija) (v nadaljevanju: CSDD) nalaga, da javnosti omogoči dostop do podatkov v zvezi s kazenskimi točkami, izrečenimi voznikom za cestnoprometne prekrške, ne da bi morala oseba, ki dostop zahteva, izkazati poseben interes za njihovo pridobitev. Ugotovilo je, da nujnost posredovanja osebnih podatkov v zvezi z kazenskimi točkami, naloženimi zaradi storitve cestnoprometnih prekrškov – zlasti z vidika uresničitve cilja izboljšanja varnosti v cestnem prometu, na katerega se je sklicevala latvijska vlada – ni izkazana. Poleg tega v skladu z ugotovitvami Sodišča niti pravica javnosti do dostopa do uradnih dokumentov niti pravica do svobode obveščanja ne upravičujeta take ureditve (točke 113, od 120 do 122 in točka 2 izreka).

V tem okviru je Sodišče poudarilo, da je izboljšanje prometne varnosti, ki je vključeno v latvijsko ureditev, cilj splošnega interesa, ki ga Unija priznava, in da lahko zato države članice varnost v cestnem prometu opredelijo kot „nalogo v javnem interesu".[38] Vendar nujnost latvijske ureditve posredovanja osebnih podatkov v zvezi s kazenskimi točkami za uresničitev zastavljenega cilja ni izkazana. Po eni strani ima namreč latvijski zakonodajalec na voljo številne možnosti, ki bi mu omogočale, da ta cilj uresniči z drugimi sredstvi, ki manj posegajo v temeljne pravice posameznikov, na katere se osebni podatki nanašajo. Po drugi strani je treba upoštevati občutljivost podatkov v zvezi s kazenskimi točkami in dejstvo, da lahko njihovo posredovanje javnosti pomeni resen poseg v pravici do spoštovanja zasebnega življenja in varstva osebnih podatkov, saj lahko povzroči neodobravanje družbe in stigmatizacijo posameznika, na katerega se osebni podatki nanašajo (točke od 109 do 113).

Poleg tega je Sodišče ugotovilo, da ob upoštevanju občutljivosti teh podatkov in teže tega posega v ti temeljni pravici ti pravici prevladata tako nad interesom javnosti, da ima dostop do uradnih dokumentov, kot je nacionalni register vozil in njihovih voznikov, kot nad pravico do svobode obveščanja (točki 120 in 121).

Sodišče je prav tako iz enakih razlogov razsodilo, da Splošna uredba o varstvu podatkov nasprotuje latvijski ureditvi tudi v delu, v katerem je CSDD dovoljeno, da podatke v zvezi s kazenskimi točkami, izrečenimi voznikom za cestnoprometne prekrške, posreduje gospodarskim subjektom, da bi jih ti lahko ponovno uporabili in jih posredovali javnosti (točka 126 in točka 3 izreka).

Sodišče je nazadnje pojasnilo, da načelo primarnosti prava Unije nasprotuje temu, da se predložitveno sodišče, ki odloča o pravnem sredstvu zoper latvijsko ureditev, ki jo je Sodišče opredelilo za nezdružljivo s pravom Unije, odloči, da se pravni učinki te ureditve ohranijo do dneva razglasitve pravnomočne sodbe predložitvenega sodišča (točka 137 in točka 4 izreka).

III. Obdelava osebnih podatkov v smislu Direktive 2002/58

[38] V skladu s členom 6(1)(e) Splošne uredbe o varstvu podatkov je obdelava osebnih podatkov zakonita, če je „potrebna za opravljanje naloge v javnem interesu […]".

Sodba z dne 2. oktobra 2018 (veliki senat), Ministerio Fiscal (C-207/16, ECLI:EU:C:2018:788)[39]

V obravnavani zadevi je španski preiskovalni sodnik zavrnil predlog, podan v okviru preiskave ropa, v katerem sta bila ukradena denarnica in mobilni telefon. Natančneje, kriminalistična policija je pri navedenem sodniku vložila predlog, naj ji za obdobje dvanajstih dni od ropa odobri dostop do identifikacijskih podatkov uporabnikov telefonskih številk, ki so bile aktivirane z ukradenega telefona. Ta predlog je bil zavrnjen z obrazložitvijo, da dejstva, na katera se je nanašala kazenska preiskava, niso pomenila „hudega“ kaznivega dejanja – ki je po španskem pravu kaznivo dejanje, ki se kaznuje s kaznijo več kot pet let zapora – dostop do identifikacijskih podatkov pa se lahko odobri samo za tovrstna kazniva dejanja.

Sodišče je najprej opozorilo, da dostop javnih organov do osebnih podatkov, ki jih hranijo ponudniki elektronskih komunikacijskih storitev, v okviru kazenske preiskave spada na področje uporabe Direktive 2002/58, nato pa razsodilo, da dostop do identifikacijskih podatkov imetnikov kartic SIM, aktiviranih z ukradenim mobilnim telefonom, kot so priimek, ime in po potrebi naslov teh imetnikov, pomeni poseg v temeljni pravici do spoštovanja zasebnega življenja in do varstva osebnih podatkov, ki sta zagotovljeni z Listino, tudi če ni okoliščin, ki bi omogočale opredelitev tega posega kot „hudega”, in ne da bi bilo pomembno, ali so zadevne informacije o zasebnem življenju občutljive, niti ali so zadevnim osebam zaradi navedenega posega morda nastale nevšečnosti. Vendar je Sodišče poudarilo, da ta poseg ni tako hud, da bi moral biti ta dostop na področju preprečevanja, preiskovanja, odkrivanja in pregona kaznivih dejanj omejen na boj proti hudim kaznivim dejanjem. Sodišče je navedlo, da so sicer v Direktivi 2002/58 taksativno našteti cilji, ki lahko upravičijo nacionalno ureditev, ki ureja dostop javnih organov do zadevnih podatkov in tako odstopa od načela zaupnosti elektronskih komunikacij, pri čemer mora ta dostop dejansko in strogo ustrezati kateremu od teh ciljev, vendar da – kar zadeva cilj preprečevanja, preiskovanja, odkrivanja in pregona kaznivih dejanj – v besedilu Direktive 2002/58 ta cilj ni omejen na boj proti zgolj hudim kaznivim dejanjem, ampak se nanaša na „kazniva dejanja” na splošno (točke 38, 42 in od 59 do 63 ter izrek).

Sodišče je v tem okviru pojasnilo, da je sicer v sodbi *Tele2 Sverige ter Watson in drugi*[40] razsodilo, da lahko le boj proti hudemu kriminalu upraviči dostop javnih organov do osebnih podatkov, ki jih hranijo ponudniki elektronskih komunikacijskih storitev ter na podlagi celote katerih je mogoče izpeljati natančne ugotovitve o zasebnem življenju oseb, za katerih podatke gre, vendar je bila ta razlaga utemeljena s tem, da mora biti cilj, ki se uresničuje z ureditvijo, ki ta dostop ureja, povezan s težo posega v zadevne temeljne pravice, ki ga povzroči ta ukrep. Tako lahko v skladu z načelom sorazmernosti na tem področju hud poseg upraviči le cilj boja proti kriminalu, ki mora biti prav tako opredeljen kot „hud”. Nasprotno, kadar poseg, ki ga pomeni tak dostop, ni hud, se navedeni dostop lahko upraviči s ciljem preprečevanja, preiskovanja, odkrivanja in pregona „kaznivih dejanj” na splošno (točke od 54 do 57).

Sodišče je v obravnavani zadevi štelo, da dostopa le do podatkov, na katere se nanaša zadevni predlog, ni mogoče opredeliti kot „hud” poseg v temeljne pravice oseb, za katerih podatke gre, ker ti podatki ne omogočajo izpeljave natančnih ugotovitev o njihovem zasebnem življenju. Sodišče je na podlagi tega ugotovilo, da se poseg, ki ga pomeni dostop do takih podatkov, torej

[39] Ta sodba je bila predstavljena v Letnem poročilu 2018, str. 81 in 82.
[40] Sodba Sodišča z dne 21. decembra 2016, *Tele2 Sverige ter Watson in drugi* (C-203/15 in C-698/15, EU:C:2016:970).

lahko upraviči s ciljem preprečevanja, preiskovanja, odkrivanja in pregona „kaznivih dejanj" na splošno, ne da bi bilo potrebno, da so ta kazniva dejanja opredeljena kot „huda" (točki 61 in 62).

Sodbi z dne 6. oktobra 2020 (veliki senat), Privacy International (C-623/17, EU:C:2020:790) ter La Quadrature du Net in drugi (C-511/18, C-512/18 in C-520/18, EU:C:2020:791)[41]

Sodna praksa v zvezi s hrambo osebnih podatkov in dostopom do njih na področju elektronskih komunikacij, zlasti sodba Tele2 Sverige ter Watson in drugi, v kateri je Sodišče med drugim razsodilo, da države članice ponudnikom elektronskih komunikacijskih storitev ne morejo naložiti obveznosti splošne in neselektivne hrambe podatkov o prometu in lokaciji, je pri nekaterih državah vzbudila pomisleke in bojazen, da so prikrajšane za instrument, ki je po njihovem mnenju potreben za zaščito nacionalne varnosti in boj proti kriminalu.

V tem okviru so bili Investigatory Powers Tribunal (sodišče s preiskovalnimi pooblastili, Združeno kraljestvo) (zadeva Privacy International, C-623/17), Conseil d'État (državni svet, Francija) (združeni zadevi La Quadrature du Net in drugi, C-511/18 in C-512/18)) in Cour constitutionnelle (ustavno sodišče, Belgija) (zadeva Ordre des barreaux francophones et germanophone in drugi, C-520/18) predloženi spori v zvezi z zakonitostjo ureditev, ki so jih sprejele nekatere države članice na teh področjih in s katerimi je določena predvsem obveznost ponudnikov elektronskih komunikacijskih storitev, da javnemu organu posredujejo podatke uporabnikov o prometu in lokaciji ali pa da te podatke splošno ali neselektivno hranijo.

Sodišče je v dveh sodbah, ki ju je izdalo 6. oktobra 2020 v velikem senatu, najprej razsodilo, da nacionalne ureditve, s katerimi je ponudnikom elektronskih komunikacijskih storitev naloženo, da podatke o prometu in lokaciji hranijo ali pa da te podatke v ta namen posredujejo nacionalnim varnostnim in obveščevalnim organom, spadajo na področje uporabe Direktive 2002/58 (točka 49 in točka 1 izreka sodbe Privacy International ter točka 104 sodbe La Quadrature du Net in drugi).

Dalje, Sodišče je opozorilo, da Direktiva 2002/58[42] ne omogoča, da bi odstopanje od načelne obveznosti zagotavljanja zaupnosti elektronskih komunikacij in z njimi povezanih podatkov ter od prepovedi shranjevanja teh podatkov postalo pravilo. To pomeni, da ta direktiva državam članicam omogoča, da med drugim zaradi nacionalne varnosti sprejmejo zakonske ukrepe, s katerimi omejijo obseg pravic in obveznosti, določenih s to direktivo, zlasti obveznosti zagotavljanja zaupnosti sporočil in podatkov o prometu,[43] le ob upoštevanju splošnih načel prava Unije, med katerimi je načelo sorazmernosti, in temeljnih pravic, zagotovljenih z Listino[44] (točki 59 in 60 sodbe Privacy International ter točki 111 in 113 sodbe La Quadrature du Net in drugi).

V tem okviru je Sodišče po eni strani v zadevi Privacy International ugotovilo, da Direktiva 2002/58, razlagana ob upoštevanju Listine, nasprotuje nacionalni ureditvi, s katero je ponudnikom elektronskih komunikacijskih storitev zaradi zaščite nacionalne varnosti naloženo

41 Ti sodbi sta bili predstavljeni v Letnem poročilu 2020, str. od 27 do 29.

42 Člen 15(1) in (3) Direktive 2002/58.

43 Člen 5(1) Direktive 2002/58.

44 Zlasti členi 7, 8 in 11 ter člen 52(1) Listine.

splošno in neselektivno posredovanje podatkov o prometu in lokaciji varnostnim in obveščevalnim službam. Po drugi strani je Sodišče v združenih zadevah La Quadrature du Net in drugi ter v zadevi Ordre des barreaux francophones et germanophone in drugi ugotovilo, da ta direktiva nasprotuje zakonskim ukrepom, s katerimi je ponudnikom elektronskih komunikacijskih storitev preventivno naložena splošna in neselektivna hramba podatkov o prometu in lokaciji.

Ti obveznosti splošnega in neselektivnega posredovanja in hrambe takih podatkov namreč pomenita posebej resno poseganje v temeljne pravice, zagotovljene z Listino, ne da bi bilo ravnanje oseb, za podatke katerih gre, kakor koli povezano s ciljem, ki mu sledi zadevna ureditev. Podobno je Sodišče razložilo člen 23(1) Splošne uredbe o varstvu podatkov v povezavi z Listino tako, da nasprotuje nacionalni ureditvi, s katero je ponudnikom dostopa do javnih spletnih komunikacijskih storitev in ponudnikom storitev gostovanja naložena splošna in neselektivna hramba med drugim osebnih podatkov v zvezi s temi storitvami (točki 71 in 82 ter točka 2 izreka sodbe Privacy International ter točke 146, 168, 174, 177 in 212 ter točki 1 in 3 izreka sodbe La Quadrature du Net in drugi).

Sodišče pa je ugotovilo, da v položajih, ko se zadevna država članica spopada z resno grožnjo nacionalni varnosti, ki se izkaže za resnično in sedanjo ali predvidljivo, Direktiva 2002/58 v povezavi z Listino ne nasprotuje temu, da se ponudnikom elektronskih komunikacijskih storitev odredi splošna in neselektivna hramba podatkov o prometu in lokaciji. V zvezi s tem je Sodišče pojasnilo, da mora biti sklep o tej odredbi za obdobje, katerega trajanje je omejeno na to, kar je nujno potrebno, predmet učinkovitega nadzora s strani sodišča ali neodvisnega upravnega organa, katerega odločitev je zavezujoča, da se preveri obstoj enega od teh položajev, pa tudi spoštovanje določenih pogojev in jamstev. V teh okoliščinah navedena direktiva prav tako ne nasprotuje avtomatizirani analizi podatkov, med drugim podatkov o prometu in lokaciji, vseh uporabnikov elektronskih komunikacijskih sredstev (točke od 137 do 139 in od 177 do 179 ter točki 1 in 2 izreka sodbe La Quadrature du Net in drugi).

Sodišče je dodalo, da Direktiva 2002/58 v povezavi z Listino ne nasprotuje zakonskim ukrepom, ki omogočajo ciljno hrambo – za obdobje, katerega trajanje je omejeno na to, kar je nujno potrebno – podatkov o prometu in lokaciji, ki je na podlagi objektivnih in nediskriminatornih elementov omejena glede na kategorije zadevnih oseb ali z geografskim merilom. Ta direktiva prav tako ne nasprotuje takim ukrepom, ki določajo splošno in neselektivno hrambo naslovov IP, dodeljenih viru sporočila, če je obdobje hrambe omejeno na to, kar je nujno potrebno, niti ukrepom, ki določajo takšno hrambo podatkov o civilni identiteti uporabnikov elektronskih komunikacijskih sredstev, pri čemer države članice hrambe v zadnjenavedenem primeru niso dolžne časovno omejiti. Poleg tega navedena direktiva ne nasprotuje zakonskemu ukrepu, ki omogoča takojšnjo hrambo podatkov, s katerimi razpolagajo ponudniki storitev, v položajih, ko se pojavi potreba po tem, da se ti podatki hranijo dlje, kot je zakonsko določeno, zaradi razjasnitve hudih kaznivih dejanj ali groženj nacionalni varnosti, če so bila ta kazniva dejanja ali grožnje že ugotovljene ali je mogoče utemeljeno domnevati, da obstajajo (točke 161, 163 in 168 ter točka 1 izreka sodbe La Quadrature du Net in drugi).

Sodišče je še razsodilo, da Direktiva 2002/58 v povezavi z Listino ne nasprotuje nacionalni ureditvi, s katero je ponudnikom elektronskih komunikacijskih storitev naloženo, da zbirajo med drugim podatke o prometu in lokaciji v realnem času, kadar je to zbiranje omejeno na osebe, v zvezi s katerimi obstaja utemeljen razlog za sum, da so tako ali drugače vpletene v teroristične dejavnosti, in je predmet predhodnega nadzora, ki ga izvaja sodišče ali neodvisen upravni organ,

katerega odločitev je zavezujoča, da se zagotovi, da je takšno zbiranje v realnem času dovoljeno samo v mejah tega, kar je nujno potrebno. V nujnem primeru se mora nadzor izvesti v najkrajšem možnem času (točka 192 in točka 2 izreka sodbe La Quadrature du Net in drugi).

Nazadnje, Sodišče je obravnavalo vprašanje časovne ohranitve učinkov nacionalne ureditve, za katero je bilo ugotovljeno, da ni v skladu s pravom Unije. V zvezi s tem je razsodilo, da nacionalno sodišče ne more uporabiti določbe nacionalnega prava, na podlagi katere lahko časovno omeji učinke ugotovitve nezakonitosti, ki jo mora sprejeti, v zvezi z nacionalno ureditvijo, s katero je ponudnikom elektronskih komunikacijskih storitev naložena splošna in neselektivna hramba podatkov o prometu in lokaciji ter za katero je bilo ugotovljeno, da ni skladna z Direktivo 2002/58, razlagano ob upoštevanju Listine.

Sodišče je ob upoštevanju navedenega in da bi dalo koristen odgovor nacionalnemu sodišču, opozorilo, da glede na sedanje stanje prava Unije dopustnost in presoja dokazov, pridobljenih s hrambo podatkov, ki je v nasprotju s pravom Unije, v okviru kazenskega postopka zoper osebe, osumljene hudih kaznivih dejanj, spadata izključno na področje uporabe nacionalnega prava. Vendar je Sodišče pojasnilo, da se z Direktivo 2002/58, razlagano ob upoštevanju načela učinkovitosti, zahteva, da nacionalno kazensko sodišče v okviru takšnega kazenskega postopka zavrne dokaze, pridobljene s splošno in neselektivno hrambo podatkov o prometu in lokaciji, ki ni v skladu s pravom Unije, če se osebe, osumljene kaznivih dejanj, ne morejo učinkovito opredeliti glede teh dokazov (točki 222 in 228 ter točka 4 izreka sodbe La Quadrature du Net in drugi).

Sodba z dne 2. marca 2021 (veliki senat), Prokuratuur (Pogoji za dostop do podatkov o elektronskih komunikacijah) (C-746/18, EU:C:2021:152)

Zoper H. K. je bil v Estoniji sprožen kazenski postopek zaradi tatvine, uporabe bančne kartice druge osebe in nasilja nad udeleženci sodnega postopka. Oseba H. K. je bila zaradi teh kaznivih dejanj na prvi stopnji obsojena na zaporno kazen dveh let. Ta odločba je bila v pritožbenem postopku potrjena. Zapisniki, na katere se opira ugotovitev, da so bila ta kazniva dejanja izvršena, so bili sestavljeni zlasti na podlagi osebnih podatkov, ki so bili pridobljeni v okviru zagotavljanja elektronskih komunikacijskih storitev. Riigikohus (vrhovno sodišče, Estonija), pri katerem je oseba H. K. vložila kasacijsko pritožbo, je izrazilo dvome glede združljivosti pogojev, pod katerimi so imele preiskovalne službe dostop do teh podatkov, s pravom Unije.[45]

Ti dvomi so se nanašali, prvič, na vprašanje, ali je dolžina obdobja, za katero so imele preiskovalne službe dostop do podatkov, upoštevna kot merilo, na podlagi katerega je mogoče oceniti težo s tem dostopom izvršenega posega v temeljne pravice posameznikov, na katere se nanašajo osebni podatki. Če je to obdobje zelo kratko ali če je količina zbranih podatkov zelo majhna, se je predložitveno sodišče tako spraševalo, ali se lahko tak poseg upraviči tudi s ciljem boja proti kriminalu na splošno, in ne samo s ciljem boja proti hudemu kriminalu. Drugič, predložitveno sodišče je želelo izvedeti, ali je mogoče estonsko državno tožilstvo, ob upoštevanju različnih nalog, ki so mu zaupane z nacionalno zakonodajo, šteti za „neodvisen“

[45] Natančneje s členom 15(1) Direktive 2002/58 v povezavi s členi 7, 11 in 52(1) Listine.

upravni organ v smislu sodbe Tele2 Sverige ter Watson in drugi,[46] ki lahko preiskovalnemu organu dovoli dostop do zadevnih podatkov.

Sodišče je v sodbi, ki jo je izrekel veliki senat, razsodilo, da Direktiva 2002/58 v povezavi z Listino nasprotuje nacionalni ureditvi, ki javnim organom zaradi preprečevanja, preiskovanja, odkrivanja in pregona kaznivih dejanj omogoča dostop do podatkov o prometu ali lokaciji, iz katerih bi bile lahko razvidne informacije o komunikacijah, ki jih je uporabnik opravil z uporabo elektronskih komunikacijskih sredstev, ali o lokaciji uporabljene terminalske opreme, in iz katerih bi bilo mogoče natančno sklepati o njegovem zasebnem življenju, ne da bi bil ta dostop omejen na postopke, povezane z bojem proti hudemu kriminalu ali preprečevanju resnih groženj javni varnosti. V skladu z ugotovitvami Sodišča trajanje obdobja, za katero se zahteva dostop do teh podatkov, in količina ali vrsta podatkov, ki so na voljo za to obdobje, ne vpliva na to ugotovitev. Poleg tega je Sodišče štelo, da ista direktiva v povezavi z Listino nasprotuje nacionalni ureditvi, ki državnemu tožilstvu podeljuje pristojnost, da javnemu organu zaradi preiskovanja kaznivih dejanj dovoli dostop do podatkov o prometu in lokaciji (točki 45 in 59 ter točki 1 in 2 izreka).

V zvezi s ciljem preprečevanja, preiskovanja, odkrivanja in pregona kaznivih dejanj, ki se je želel doseči z zadevno ureditvijo, je Sodišče ob upoštevanju načela sorazmernosti ugotovilo, da se lahko dostop javnih organov do vseh podatkov o prometu ali lokaciji, ki omogočajo natančne ugotovitve v zvezi z zasebnim življenjem posameznikov, na katere se nanašajo osebni podatki, upraviči samo s ciljema boja proti hudemu kriminalu in preprečevanja hudih nevarnosti za javno varnost, ne da bi lahko drugi dejavniki, povezani s sorazmernostjo zahteve za dostop, kot je trajanje obdobja, za katero se zahteva dostop do takih podatkov, učinkovali tako, da bi bilo mogoče tak dostop upravičiti s ciljem preprečevanja, preiskovanja, odkrivanja in pregona kaznivih dejanj na splošno (točki 33 in 35).

Glede pristojnosti državnega tožilstva, da v okviru usmerjanja kazenske preiskave dovoli dostop javnega organa do podatkov o prometu in lokaciji, je Sodišče spomnilo, da je treba pogoje, pod katerimi morajo ponudniki elektronskih komunikacijskih storitev pristojnim nacionalnim organom omogočiti dostop do podatkov, s katerimi razpolagajo, določiti v nacionalnem pravu. Vendar mora taka ureditev, da bi izpolnjevala zahtevo po sorazmernosti, vsebovati jasna in natančna pravila, ki urejajo obseg in izvajanje zadevnega ukrepa ter določajo minimalne zahteve, tako da imajo posamezniki, na katere se nanašajo osebni podatki, na voljo zadostna jamstva, ki omogočajo učinkovito varovanje teh podatkov pred tveganji zlorab. Ta ureditev mora biti zakonsko zavezujoča v nacionalnem pravu, v njej pa mora biti navedeno, v kakšnih okoliščinah in pod katerimi materialnimi in procesnimi pogoji je mogoče sprejeti ukrep, ki določa obdelavo takih podatkov, s čimer se tako zagotovi, da je poseganje omejeno na to, kar je nujno potrebno (točka 48).

Da bi se v praksi zagotovilo popolno spoštovanje teh pogojev, je, kot je navedlo Sodišče, bistveno, da pred dostopom pristojnih nacionalnih organov do hranjenih podatkov sodišče ali neodvisen upravni organ opravi predhoden preizkus in da se odločba tega sodišča ali tega organa izda na obrazložen predlog teh nacionalnih organov, ki se predloži, med drugim, v okviru postopkov preprečevanja, odkrivanja ali pregona kaznivih dejanj. V primeru ustrezno utemeljene nujnosti je treba preizkus opraviti v kratkih rokih (točka 51).

[46] Sodba z dne 21. decembra 2016, Tele2 Sverige ter Watson in drugi (C-203/15 in C-698/15, EU:C:2016:970, točka 120).

Glede tega je Sodišče pojasnilo, da se v zvezi s tem predhodnim preizkusom med drugim zahteva, da ima sodišče ali organ, ki je zadolžen za izvedbo tega preizkusa, vse pristojnosti in zagotavlja vsa potrebna jamstva za uskladitev različnih zadevnih interesov in pravic. Glede, natančneje, preiskave kaznivih dejanj mora to sodišče ali ta organ v okviru takega preizkusa zagotoviti pravično ravnotežje med interesi, povezanimi s potrebami preiskave, ki se nanaša na boj proti kriminalu, na eni strani ter temeljnimi pravicami do spoštovanja zasebnega življenja in varstva osebnih podatkov posameznikov, do katerih podatkov se dostopa, na drugi. Če tega preizkusa ne izvaja sodišče, ampak neodvisen upravni organ, mora imeti ta organ status, ki mu omogoča, da pri izvajanju svojih nalog deluje objektivno in nepristransko, pri čemer mora biti zato zaščiten pred kakršnim koli zunanjim vplivom (točki 52 in 53).

V skladu z ugotovitvami Sodišča iz zahteve po neodvisnosti, ki jo mora izpolnjevati organ, pristojen za izvajanje predhodnega preizkusa, izhaja, da mora imeti ta organ v razmerju do organa, ki zahteva dostop do podatkov, status tretje osebe, tako da lahko prvonavedeni organ ta preizkus izvede objektivno in nepristransko, brez kakršnega koli zunanjega vpliva. Natančneje, na kazenskem področju zahteva po neodvisnosti pomeni, da organ, pristojen za ta predhodni preizkus, prvič, ne sodeluje pri preiskovanju zadevnih kaznivih dejanj, in drugič, da je v razmerju do strank v kazenskem postopku nevtralen. To pa za državno tožilstvo, kot je estonsko državno tožilstvo, ki usmerja preiskovalni postopek in po potrebi zastopa obtožbo, ne velja. Iz tega sledi, da državno tožilstvo ne sme opravljati omenjenega predhodnega preizkusa (točke 54, 55 in 57).

IV. Prenos osebnih podatkov v tretje države

Sodba z dne 6. novembra 2003 (veliki senat), Lindqvist (C-101/01, EU:C:2003:596)[47]

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, 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 na eni strani in nevključitve 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

[47] Ta sodba je bila predstavljena v Letnem poročilu 2003, str. 67.

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)[48]

M. Schrems, avstrijski državljan in uporabnik družbenega omrežja Facebook, je pri Data Protection Commissioner (pooblaščenec za varstvo podatkov, Irska) vložil pritožbo, ker je družba Facebook Ireland osebne podatke svojih uporabnikov prenašala v Združene države in jih hranila 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/ES[49] ugotovila, da Združene države v okviru sistema „varnega pristana" (angleško „safe harbour"),[50] 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, 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, ki jo je Komisija sprejela na podlagi navedenega člena 25(6) Direktive 95/46.

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 tega ni storila, člen 1 te odločbe krši zahteve, določene v členu 25(6) Direktive 95/46, razlagane ob upoštevanju Listine, in zato ni veljaven. Načela „varnega pristana" se namreč uporabljajo zgolj za samocertificirane ameriške organizacije, ki prejemajo osebne podatke iz Unije, ne zahteva pa se, da tudi ameriški javni organi spoštujejo navedena načela. Poleg tega Odločba 2000/520 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 bil ugotovljen obstoj učinkovitega sodnega varstva v primeru takih posegov (točke 82, od 87 do 89 in od 96 do 98 ter točka 2 izreka).

Sodišče je poleg tega ugotovilo, da člen 3 Odločbe 2000/ni veljaven, ker nacionalnim nadzornim organom odvzema pooblastila, ki jih imajo na podlagi člena 28 Direktive 95/46, 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 vpliva na veljavnost te odločbe v celoti (točki 105 in 106).

---

[48] Ta sodba je bila predstavljena v Letnem poročilu 2015, p. 48.

[49] 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).

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

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 popravo 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 v 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).

Sodba z dne 16. julija 2020 (veliki senat), Facebook Ireland in Schrems (C-311/18, ECLI:EU:C:2015:650)[51]

Splošna uredba o varstvu podatkov določa, da se taki podatki v tretjo državo načeloma lahko prenesejo le, če ta tretja država zagotavlja ustrezno raven varstva teh podatkov. Ta uredba določa, da lahko Komisija ugotovi, da neka tretja država zaradi svoje domače zakonodaje ali mednarodnih obveznosti zagotavlja ustrezno raven varstva.[52] Če tak sklep o ustreznosti ni sprejet, se tak prenos lahko opravi le, če izvoznik osebnih podatkov, ki ima sedež v Uniji, predvidi ustrezne zaščitne ukrepe, ki se lahko med drugim zagotovijo s standardnimi določili o varstvu podatkov, ki jih sprejme Komisija, in če imajo posamezniki, na katere se osebni podatki nanašajo, na voljo izvršljive pravice in učinkovita pravna sredstva.[53] Poleg tega Splošna uredba o varstvu podatkov natančno določa pogoje, pod katerimi je tak prenos mogoč, če ni bil sprejet sklep o ustreznosti ali niso bili zagotovljeni ustrezni zaščitni ukrepi.[54]

Maximillian Schrems, avstrijski državljan, ki prebiva v Avstriji, od leta 2008 uporablja Facebook. Enako kot velja za druge uporabnike, ki prebivajo v Uniji, družba Facebook Ireland osebne podatke M. Schremsa v celoti ali delno prenaša na strežnike družbe Facebook Inc., ki so na ozemlju Združenih držav, kjer se ti podatki obdelujejo. M. Schrems je pri irskem nadzornem organu vložil pritožbo, v kateri je v bistvu predlagal, naj se ti prenosi prepovejo. Trdil je, da zakonodaja in praksa v Združenih državah ne zagotavljata zadostnega varstva podatkov, ki so bili preneseni v to državo, pred tem, da bi do njih dostopali javni organi. Ta pritožba je bila

51 Ta sodba je bila predstavljena v Letnem poročilu 2020, str. od 24 do 27.
52 Člen 45 Splošne uredbe o varstvu podatkov.
53 Člen 46(1) in (2)(c) Splošne uredbe o varstvu podatkov.
54 Člen 49 Splošne uredbe o varstvu podatkov.

zavrnjena med drugim zato, ker je Komisija v Odločbi 2000/520[55] ugotovila, da Združene države zagotavljajo ustrezno raven varstva. Sodišče je s sodbo z dne 6. oktobra 2015 na podlagi vprašanja za predhodno odločanje, ki mu ga je predložilo High Court (višje sodišče, Irska), to odločbo razglasilo za neveljavno (v nadaljevanju: sodba Schrems I)[56] (točki 52 in 53).

Po tem, ko je bila izdana sodba Schrems I in je nato irsko sodišče razveljavilo odločbo, s katero je bila pritožba M. Schremsa zavrnjena, je irski nadzorni organ M. Schremsa pozval, naj pritožbo spremeni tako, da upošteva dejstvo, da je Sodišče Odločbo 2000/520 razglasilo za neveljavno. M. Schrems je v spremenjeni pritožbi še naprej trdil, da Združene države ne zagotavljajo zadostnega varstva osebnih podatkov, ki so bili preneseni v to državo. Predlagal je, naj se za naprej prepove ali začasno ustavi prenos njegovih osebnih podatkov iz Unije v Združene države, ki ga družba Facebook Ireland odslej opravlja na podlagi standardnih določil o varstvu podatkov iz Priloge k Sklepu 2010/87/EU[57]. Irski nadzorni organ je menil, da je odločitev o pritožbi M. Schremsa med drugim odvisna od veljavnosti Sklepa 2010/87, zato je začel postopek pred High Court (višje sodišče) z namenom, da bi to sodišče pri Sodišču vložilo predlog za sprejetje predhodne odločbe. Po začetku tega postopka je Komisija sprejela Sklep (EU) 2016/1250 o ustreznosti varstva, ki ga zagotavlja zasebnostni ščit EU-ZDA[58] (točke 54, 55 in 57).

Predložitveno sodišče je v predlogu za sprejetje predhodne odločbe Sodišče spraševalo o uporabi Splošne uredbe o varstvu podatkov za prenose osebnih podatkov na podlagi standardnih določil o varstvu podatkov iz Sklepa 2010/87, o ravni varstva, ki se s to uredbo zahteva za take prenose, in o obveznostih, ki jih imajo v zvezi s tem nadzorni organi. Poleg tega je High Court postavilo vprašanje o veljavnosti Sklepa 2010/87 in Sklepa 2016/1250.

Sodišče je ugotovilo, da pri preučitvi Sklepa 2010/87 z vidika Listine ni bil ugotovljen noben element, ki bi lahko vplival na njegovo veljavnost. V zvezi s Sklepom 2016/1250 pa je ugotovilo, da ta sklep ni veljaven (točki 4 in 5 izreka).

Sodišče je najprej ugotovilo, da se pravo Unije, med drugim tudi Splošna uredba o varstvu podatkov, uporablja za prenos osebnih podatkov, ki ga gospodarski subjekt s sedežem v državi članici v komercialne namene opravi drugemu gospodarskemu subjektu s sedežem v tretji državi, ne glede na to, da lahko organi te tretje države te podatke med tem prenosom ali po njem obdelujejo za namene javne varnosti, obrambe in državne varnosti. Pojasnilo je, da to, da organi tretje države podatke obdelujejo na tak način, še ne pomeni, da je tak prenos izključen iz področja uporabe te uredbe (točke 86, 88 in 89 ter točka 1 izreka).

Kar zadeva raven varstva, ki se zahteva pri takem prenosu, je Sodišče razsodilo, da je treba zahteve, ki jih v zvezi s tem vsebuje Splošna uredba o varstvu podatkov ter se nanašajo na

---

55 Odločba Komisije z dne 26. julija 2000 po Direktivi 95/46 Evropskega parlamenta in Sveta 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).

56 Sodba Sodišča z dne 6. oktobra 2015, Schrems, C-362/14, EU:C:2015:650 (glej tudi Sporočilo za medije št. 117/15).

57 Sklep Komisije z dne 5. februarja 2010 o standardnih pogodbenih klavzulah za prenos osebnih podatkov obdelovalcem s sedežem v tretjih državah v skladu z Direktivo Evropskega parlamenta in Sveta 95/46/ES (UL 2010, L 39, str. 5), kakor je bil spremenjen z Izvedbenim sklepom Komisije (EU) 2016/2297 z dne 16. decembra 2016 (UL 2016, L 344, str. 100).

58 Izvedbeni sklep Komisije z dne 12. julija 2016 na podlagi Direktive Evropskega parlamenta in Sveta 95/46/ES o ustreznosti varstva, ki ga zagotavlja zasebnostni ščit EU-ZDA (UL 2016, L 207, str. 1).

ustrezne zaščitne ukrepe, izvršljive pravice in učinkovita pravna sredstva, razlagati tako, da mora biti osebam, katerih osebni podatki se prenašajo v tretjo državo na podlagi standardnih določil o varstvu podatkov, zagotovljena raven varstva, ki je v bistvu enakovredna ravni varstva, ki se v Uniji zagotavlja s to uredbo v povezavi z Listino. V tem okviru je pojasnilo, da je treba pri presoji te ravni varstva upoštevati tako pogodbena določila, dogovorjena med izvoznikom podatkov s sedežem v Uniji in prejemnikom prenosa s sedežem v tretji državi, kot – v zvezi z morebitnim dostopom javnih organov te tretje države do tako prenesenih osebnih podatkov – upoštevne elemente pravnega sistema te države (točka 105 in točka 2 izreka).

Glede obveznosti nadzornih organov v okviru takega prenosa je Sodišče razsodilo, da mora tak organ, razen če obstaja sklep o ustreznosti, ki ga je veljavno sprejela Komisija, med drugim začasno ustaviti ali prepovedati prenos osebnih podatkov v tretjo državo, če glede na vse okoliščine tega prenosa meni, da standardna določila o varstvu podatkov v tej tretji državi niso ali ne morejo biti spoštovana in da varstva prenesenih podatkov, ki se zahteva s pravom Unije, ni mogoče zagotoviti na noben drug način, kadar izvoznik podatkov s sedežem v Uniji ni sam začasno ustavil prenosa ali z njim prenehal (točka 121 in točka 3 izreka).

Sodišče je nato preučilo veljavnost Sklepa 2010/87. Sodišče je navedlo, da samo zaradi tega, ker standardna določila o varstvu podatkov iz tega sklepa zaradi njihove pogodbene narave ne zavezujejo organov tretjih držav, v katere se lahko podatki posredujejo, ta sklep še ni neveljaven. Nasprotno je veljavnost tega sklepa, kot je pojasnilo, odvisna od tega, ali ta vsebuje učinkovite mehanizme, ki v praksi omogočajo, da se zagotovi raven varstva, ki se zahteva s pravom Unije, in to, da se prenosi osebnih podatkov, ki temeljijo na takih določilih, v primeru kršitve teh določil ali v primeru, da jih ni mogoče spoštovati, začasno ustavijo ali prepovejo. Sodišče je ugotovilo, da so s Sklepom 2010/87 taki mehanizmi vzpostavljeni. V zvezi s tem je med drugim poudarilo, da je s tem sklepom vzpostavljena obveznost izvoznika podatkov in njihovega prejemnika, da predhodno preverita, ali se v zadevni tretji državi ta raven varstva spoštuje, in da ta sklep tega prejemnika zavezuje, da izvoznika podatkov obvesti o svoji morebitni nezmožnosti spoštovanja standardnih določil o varstvu podatkov, slednji pa mora v tem primeru začasno ustaviti prenos podatkov in/ali odstopiti od pogodbe s prejemnikom (točke 132, 136, 137, 142 in 148 ter točka 4 izreka).

Nazadnje je Sodišče preučilo veljavnost Sklepa 2016/1250 glede na zahteve, ki izhajajo iz Splošne uredbe o varstvu podatkov, ob upoštevanju določb Listine, s katerimi se zagotavljajo spoštovanje zasebnega in družinskega življenja, varstvo osebnih podatkov in pravica do učinkovitega sodnega varstva. V zvezi s tem je Sodišče ugotovilo, da se v tem sklepu, enako kot v Odločbi 2000/520, priznava primarnost zahtev, povezanih z nacionalno varnostjo, javnim interesom in spoštovanjem ameriške zakonodaje, kar omogoča posege v temeljne pravice oseb, katerih osebni podatki se prenašajo v to tretjo državo. V skladu z navedbami Sodišča omejitve varstva osebnih podatkov, ki izhajajo iz notranje ureditve Združenih držav, ki se nanaša na dostop ameriških javnih organov do takih podatkov, ki se prenesejo iz Unije v to tretjo državo, in njihovo uporabo s strani teh organov, in ki jih je Komisija ocenila v Sklepu 2016/1250, niso urejene tako, da bi izpolnjevale zahteve, ki so v bistvu enakovredne zahtevam, ki v pravu Unije izhajajo iz načela sorazmernosti, tako da ni mogoče šteti, da so programi nadzora, ki temeljijo na tej ureditvi, omejeni na tisto, kar je nujno potrebno. Na podlagi ugotovitev, navedenih v tem sklepu, je Sodišče navedlo, da v zvezi z nekaterimi programi nadzora ta ureditev ne vsebuje nikakršnih omejitev v njej vsebovanega pooblastila za izvajanje teh programov in tudi ne zaščitnih ukrepov za neameriške osebe, na katere se ti programi

lahko nanašajo. Sodišče je dodalo, da ta ureditev sicer določa zahteve, ki jih morajo ameriški organi pri izvajanju zadevnih programov nadzora spoštovati, vendar pa osebam, na katere se osebni podatki nanašajo, ne daje pravic, ki bi jih bilo mogoče zoper ameriške organe uveljavljati pred sodišči (točke 164, 165, od 180 do 182, 184 in 185).

V zvezi z zahtevo po sodnem varstvu je Sodišče – v nasprotju s stališčem Komisije iz Sklepa 2016/1250 – razsodilo, da mehanizem varuha človekovih pravic iz tega sklepa tem osebam ne zagotavlja pravnega sredstva pred organom, ki bi zagotavljal jamstva, ki so v bistvu enakovredna tistim, ki se zahtevajo s pravom Unije, tako da bi bila zagotovljena neodvisnost varuha človekovih pravic, ki se vzpostavlja s tem mehanizmom, in da bi se zagotovil obstoj pravnih pravil, na podlagi katerih bi ta varuh lahko sprejemal odločitve, ki bi bile zavezujoče za ameriške obveščevalne službe. Iz vseh teh razlogov je Sodišče ugotovilo, da Sklep 2016/1250 ni veljaven (točke od 195 do 197 in 201 ter točka 5 izreka).

V. 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.

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, 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 nezdružljiva 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)[59]

Promusicae, špansko neprofitno združenje, ki povezuje producente 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 Juzgado de lo Mercantil n° 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),[60] Direktiva 2001/29/ES o usklajevanju določenih vidikov avtorske in

[59] Ta sodba je bila predstavljena v Letnem poročilu 2008, str. 41.

[60] 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).

sorodnih pravic v informacijski družbi,[61] Direktiva 2004/48/ES o uveljavljanju pravic intelektualne lastnine[62] in Direktiva 2002/58 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 pravilnega 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 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)[63]

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, 2000/31, 2001/29, 2002/58 in 2004/48, 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, 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

[61] 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).

[62] 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).

[63] Ta sodba je bila predstavljena v Letnem poročilu 2011, str. 34.

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).

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 in 2004/48 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 zadnjenavedene 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 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 v povezavi s členom 15(1) Direktive 2002/58 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 in 2004/48 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).

Sodba z dne 17. junija 2021, M.I.C.M. (C-597/19, EU:C:2021:492)

Podjetje Mircom International Content Management & Consulting (M.I.C.M.) Limited (v nadaljevanju: Mircom) je pri Ondernemingsrechtbank Antwerpen (gospodarsko sodišče v Antwerpnu, Belgija, v nadaljevanju: predložitveno sodišče) vložilo zahtevo za posredovanje informacij, namenjeno družbi Telenet BVBA, ponudniku dostopa do interneta. S to zahtevo se je predlagalo sprejetje odločbe, s katero bi se družbi Telenet odredila predložitev identifikacijskih podatkov njenih strank na podlagi IP-naslovov, ki jih je specializirana družba zbrala za račun podjetja Mircom. Internetni priključki strank družbe Telenet so bili uporabljeni za izmenjavo filmov iz kataloga podjetja Mircom na omrežju enakovrednih partnerjev (peer-to-peer) z uporabo protokola BitTorrent. Družba Telenet je zahtevi podjetja Mircom nasprotovala.

V teh okoliščinah je predložitveno sodišče Sodišče najprej vprašalo, ali izmenjava delov podatkovne datoteke, ki vsebuje varovano delo, na navedenem omrežju pomeni priobčitev javnosti na podlagi prava Unije. Nato je želelo izvedeti, ali je imetnik pravic intelektualne lastnine, kot je podjetje Mircom, ki teh pravic ne uporablja, ampak zahteva odškodnino od domnevnih kršiteljev, upravičen do ukrepov, postopkov in pravnih sredstev, ki jih določa pravo Unije, da bi se zagotovilo spoštovanje teh pravic, na primer tako, da zahteva posredovanje informacij. Nazadnje, predložitveno sodišče je Sodišče prosilo, naj pojasni vprašanje zakonitosti, prvič, načina, kako je podjetje Mircom zbralo IP-naslove strank, in drugič, posredovanja podatkov, ki ga je podjetje Mircom zahtevalo od družbe Telenet.

Sodišče je razsodilo, da pravo Unije[64] načeloma ne nasprotuje temu, da imetnik pravic intelektualne lastnine ali tretja oseba za njegov račun sistematično beleži IP-naslove uporabnikov omrežij enakovrednih partnerjev (peer-to-peer), ki naj bi internetne priključke uporabljali pri dejanjih, ki pomenijo kršitev (predhodna obdelava podatkov), niti temu, da se temu imetniku ali tretji osebi posredujejo imena in poštni naslovi teh uporabnikov, da bi se lahko vložila odškodninska tožba (nadaljnja obdelava podatkov). Vendar morajo biti pobude in zahteve v zvezi s tem utemeljene in sorazmerne, ne smejo pomeniti zlorabe ter morajo biti določene z nacionalnim zakonodajnim ukrepom, ki omejuje obseg pravic in obveznosti, ki izhajajo iz prava Unije. Sodišče je pojasnilo, da to pravo ne določa obveznosti za družbo, kot je družba Telenet, da osebam zasebnega prava posreduje osebne podatke, zato da bi se lahko pred civilnimi sodišči začeli postopki zaradi kršitev avtorskih pravic. Vendar pravo Unije državam članicam dopušča, da tako obveznost naložijo (točke 97 in od 125 do 127 ter točka 3 izreka).

3. Odstranitev povezav do osebnih podatkov

Sodba z dne 24. septembra 2019 (veliki senat), GC in drugi (Odstranitev povezav do občutljivih podatkov) (C-136/17, ECLI:EU:C:2019:773)[65]

Sodišče (veliki senat) je v tej sodbi pojasnilo obveznosti upravljavca iskalnika v okviru zahteve za odstranitev povezav v zvezi z občutljivimi podatki.

Družba Google ni ugodila zahtevam štirih oseb za odstranitev različnih povezav na spletne strani, ki so jih objavile tretje osebe, predvsem na članke v tiskanih medijih, s seznama zadetkov, ki ga spletni iskalnik prikaže po iskanju, opravljenem na podlagi njihovega imena. Po pritožbah teh štirih oseb je Commission nationale de l'informatique et des libertés (CNIL) (nacionalna komisija za informatiko in svoboščine, Francija) zavrnila, da bi družbo Google pozvala, naj odstrani zadevne povezave. Conseil d'État (državni svet, Francija), ki mu je bila zadeva predložena, je Sodišču predlagal, naj pojasni obveznosti upravljavca iskalnika pri obravnavanju zahteve za odstranitev povezav na podlagi Direktive 95/46.

Prvič, Sodišče je opozorilo, da je obdelava osebnih podatkov, ki razkrivajo rasno ali etnično poreklo, politično mnenje, versko ali filozofsko prepričanje ali članstvo v sindikatu, in obdelava podatkov v zvezi z zdravjem ali spolnim življenjem – ob upoštevanju nekaterih izjem in odstopanj – prepovedana.[66] Obdelava podatkov v zvezi s prekrški, kazenskimi obsodbami ali varnostnimi ukrepi pa se lahko načeloma izvaja samo pod nadzorom uradnega organa ali pa če nacionalna zakonodaja določi ustrezne posebne zaščitne ukrepe[67] (točki 39 in 40).

Sodišče je razsodilo, da se prepoved in omejitve v zvezi z obdelavo teh posebnih vrst podatkov za upravljavca iskalnika uporabljajo podobno kot za vsako drugo odgovorno osebo za obdelavo osebnih podatkov. Namen teh prepovedi in omejitev je namreč zagotoviti povečano varstvo v zvezi s takimi obdelavami, ki lahko zaradi posebne občutljivosti teh podatkov pomenijo posebno

64 Člen 6(1)(f) Splošne uredbe o varstvu podatkov in člen 15(1) Direktive 2002/58.
65 Ta sodba je bila predstavljena v Letnem poročilu 2019, str. 109 in 110.
66 Člen 8(1) Direktive 95/46 in člen 9(1) Uredbe 2016/679.
67 Člen 8(5) Direktive 95/46 in člen 10 Uredbe 2016/679.

hud poseg v temeljni pravici do spoštovanja zasebnega življenja in varstva osebnih podatkov (točke od 42 do 44).

Vendar upravljavec iskalnika ni odgovoren za to, da so osebni podatki na spletni strani, ki jo je objavila tretja oseba, temveč za uvrstitev te strani na seznam zadetkov iskanja. V teh okoliščinah se prepoved in omejitve v zvezi z obdelavo občutljivih podatkov za tega upravljavca uporabljajo samo zaradi te uvrstitve na seznam zadetkov iskanja in torej prek preverjanja, ki se pod nadzorom pristojnih nacionalnih organov opravi na podlagi zahteve, ki jo vloži zadevna oseba (točki 46 in 47).

Drugič, Sodišče je štelo, da mora upravljavec iskalnika, kadar prejme zahtevo za odstranitev povezav v zvezi z občutljivimi podatki, tej zahtevi načeloma in ob upoštevanju določenih izjem ugoditi. Kar zadeva te izjeme, lahko upravljavec taki zahtevi ne ugodi zlasti, kadar ugotovi, da povezave vodijo do podatkov, ki jih je zadevna oseba očitno javno objavila,[68] če ta uvrstitev na seznam zadetkov iskanja izpolnjuje tudi vse druge pogoje glede zakonitosti obdelave osebnih podatkov in če ta oseba nima pravice, da navedeni uvrstitvi na seznam zadetkov iskanja ugovarja na podlagi razlogov, povezanih z njenim posebnim položajem[69] (točki 65 in 69).

Vsekakor mora upravljavec iskalnika, kadar prejme zahtevo za odstranitev povezav, preveriti, ali je vključitev povezave do spletne strani, na kateri so objavljeni občutljivi podatki, na seznam zadetkov, ki se prikaže po iskanju, opravljenem na podlagi imena te osebe, nujno potrebna za varovanje svobode obveščanja internetnih uporabnikov, ki bi morda imeli interes za dostop do te spletne strani na podlagi takega iskanja. Sodišče je v zvezi s tem poudarilo, da čeprav pravici do spoštovanja zasebnosti in varstva osebnih podatkov na splošno prevladata nad pravico internetnih uporabnikov do svobode obveščanja, pa je to ravnotežje lahko v posebnih primerih odvisno od narave zadevne informacije in od tega, kako občutljiva je za zasebnost zadevne osebe, ter od interesa javnosti, da razpolaga s to informacijo, ki je lahko med drugim odvisen od vloge, ki jo ima ta oseba v javnem življenju (točki 66 in 68).

Tretjič, Sodišče je razsodilo, da mora upravljavec iskalnika v okviru zahteve za odstranitev povezav v zvezi s podatki glede kazenskega sodnega postopka zoper zadevno osebo, ki se nanašajo na prejšnjo fazo tega postopka in ne ustrezajo več sedanjemu položaju, preučiti, ali ima ob upoštevanju vseh okoliščin obravnavanega primera navedena oseba pravico do tega, da zadevne informacije v sedanji fazi več ne bodo povezane z njenim imenom prek seznama zadetkov, ki se prikaže po iskanju, opravljenem na podlagi tega imena. Vendar mora upravljavec, tudi če ni tako, ker je vključitev zadevne povezave nujno potrebna za uskladitev pravic zadevne osebe do spoštovanja zasebnosti in varstva osebnih podatkov s svobodo obveščanja potencialno zainteresiranih internetnih uporabnikov, seznam zadetkov najpozneje ob prejemu zahteve za odstranitev povezav prilagoditi tako, da splošna slika, ki iz njega izhaja za internetnega uporabnika, odraža sedanje stanje sodnega postopka, za kar je med drugim potrebno, da se povezave do spletnih strani, ki vsebujejo informacije glede tega, na tem seznamu prikažejo na vrhu (točki 77 in 78).

---

68 Člen 8(2)(e) Direktive 95/46 in člen 9(2)(e) Uredbe 2016/679.
69 Člen 14, prvi odstavek, točka (a), Direktive 95/46 in člen 21(1) Uredbe 2016/679.

Sodba z dne 24. septembra 2019 (veliki senat), Google (Ozemeljski obseg odstranitve povezav) (C-507/17, ECLI:EU:C:2019:772)[70]

Commission nationale de l'informatique et des libertés (CNIL) (nacionalna komisija za informatiko in svoboščine, Francija) je družbo Google opomnila, naj v primeru, v katerem ta družba ugodi zahtevi, da se s seznama zadetkov, ki se prikaže po iskanju, opravljenem na podlagi imena posameznika, na katerega se nanašajo osebni podatki, odstranijo povezave na spletne strani, ki vsebujejo osebne podatke, ki se nanašajo na tega posameznika, povezave odstrani na vseh domenskih končnicah svojega iskalnika. Ker družba Google tega opomina ni upoštevala, ji je CNIL naložila sankcijo v višini 100.000 EUR. Conseil d'État (državni svet), pri katerem je družba Google vložila tožbo, je Sodišče zaprosil, naj pojasni ozemeljski obseg obveznosti upravljavca iskalnika, da uresniči pravico do odstranitve povezav na podlagi Direktive 95/46.

Sodišče je najprej opozorilo na možnost za posameznike, da na podlagi prava Unije uveljavljajo pravico do odstranitve povezav proti upravljavcu iskalnika, ki ima eno ali več poslovnih enot na ozemlju Unije, ne glede na to, ali je bila obdelava osebnih podatkov (v obravnavani zadevi povezave na spletne strani, na katerih so osebni podatki, ki se nanašajo na posameznika, ki uveljavlja to pravico) opravljena v Uniji.[71]

Glede obsega pravice do odstranitve povezav je Sodišče ugotovilo, da upravljavcu iskalnika povezav ni treba odstraniti na vseh različicah svojega iskalnika, ampak le na različicah svojega iskalnika, ki ustrezajo vsem državam članicam. V zvezi s tem je navedlo, da bi bil sicer z univerzalno odstranitvijo ob upoštevanju značilnosti spleta in iskalnikov v celoti dosežen cilj zakonodajalca Unije, ki je zagotavljati visoko raven varstva osebnih podatkov v celotni Uniji, vendar iz prava Unije[72] nikakor ne izhaja, da bi zakonodajalec Unije za uresničitev takega cilja določil, da se pravici do odstranitve povezav prizna obseg, ki bi presegal ozemlje držav članic. Natančneje, medtem ko pravo Unije določa mehanizme za sodelovanje med nadzornimi organi držav članic za dosego skupne odločitve, ki temelji na tehtanju pravice do spoštovanja zasebnega življenja in varstva osebnih podatkov na eni strani ter interesa javnosti iz različnih držav članic, da ima dostop do informacij, na drugi strani, taki mehanizmi trenutno niso določeni glede obsega odstranitve povezav zunaj Unije (točki 62 in 73).

V sedanjem stanju prava Unije mora upravljavec iskalnika zahtevano odstranitev povezav opraviti ne le na različici iskalnika, ki ustreza državi članici stalnega prebivališča upravičenca do te odstranitve, ampak na vseh različicah iskalnika, ki ustrezajo državam članicam, in to predvsem zato, da se zagotovi dosledna in visoka raven varstva v celotni Uniji. Poleg tega mora tak upravljavec po potrebi sprejeti ukrepe, ki so dovolj učinkoviti, da spletnim uporabnikom v Uniji preprečujejo ali jih vsaj resno odvračajo od tega, da bi do povezav, ki so predmet odstranitve, dostopali prek različice iskalnika, ki ustreza tretji državi, nacionalno sodišče pa mora preveriti, ali ukrepi, ki jih je sprejel upravljavec, to zahtevo izpolnjujejo (točka 70).

Nazadnje, Sodišče je poudarilo, da sicer pravo Unije upravljavcu iskalnika ne nalaga, da povezave odstrani na vseh različicah svojega iskalnika, vendar tega tudi ne prepoveduje. Zato so nadzorni

[70] Ta sodba je bila predstavljena v Letnem poročilu 2019, str. 111.

[71] Člen 4(1)(a) Direktive 95/46 in člen 3(1) Uredbe 2016/679.

[72] Člen 12(b) in člen 14, prvi odstavek, točka (a), Direktive 95/46 ter člen 17(1) Uredbe 2016/679.

ali sodni organi držav članic še naprej pristojni, da na podlagi nacionalnih standardov varstva temeljnih pravic opravijo tehtanje med pravico posameznika, na katerega se nanašajo osebni podatki, do spoštovanja njegovega zasebnega življenja in do varstva njegovih osebnih podatkov na eni strani ter svobodo obveščanja na drugi strani in da na koncu tega tehtanja upravljavcu tega iskalnika po potrebi odredijo, naj odstrani povezave na vseh različicah navedenega iskalnika (točki 65 in 72).

4. Privolitev uporabnika spletnega mesta v shranjevanje informacij

Sodba z dne 1. oktobra 2019 (veliki senat), Planet49 (C-673/17, ECLI:EU:C:2019:801)[73]

Sodišče je s to sodbo razsodilo, da privolitev v shranjevanje informacij ali v dostop do informacij z uporabo piškotkov, ki so nameščeni na terminalski opremi uporabnika spletnega mesta, ni veljavna, če dovoljenje izhaja iz vnaprej označenega potrditvenega okenca, in to neodvisno od tega, ali so zadevne informacije osebni podatki. Poleg tega je Sodišče pojasnilo, da mora ponudnik storitev uporabnika spletnega mesta obvestiti o času delovanja piškotkov in o tem, ali imajo lahko tretje osebe dostop do teh piškotkov.

Spor iz postopka v glavni stvari se je nanašal na organizacijo nagradne igre s strani družbe Planet49 na spletnem mestu www.dein-macbook.de. Internetni uporabniki so, da bi lahko sodelovali, morali posredovati svoje ime in naslov na spletni strani, kjer sta bili potrditveni okenci. Potrditveno okence, namenjeno dovoljenju za namestitev piškotkov, je bilo vnaprej označeno. Bundesgerichtshof (zvezno vrhovno sodišče, Nemčija), pri katerem je nemško zvezno združenje organizacij za varstvo potrošnikov vložilo pravno sredstvo, je podvomilo glede veljavnosti pridobitve privolitve uporabnikov prek vnaprej označenega potrditvenega okenca in glede obsega obveznosti obveščanja, ki je naložena ponudniku storitve.

Predlog za sprejetje predhodne odločbe se je v bistvu nanašal na razlago pojma „privolitev“ iz Direktive 2002/58[74] v povezavi z Direktivo 95/46[75] ter Splošno uredbo o varstvu podatkov[76].

Prvič, Sodišče je opozorilo, da člen 2(h) Direktive 95/46, na katerega napotuje člen 2(f) Direktive 2002/58, opredeljuje privolitev kot „vsako prostovoljno dano posebno in informirano izjavo volje, s katero posameznik, na katerega se osebni podatki nanašajo, izrazi soglasje, da se osebni podatki o njem obdelujejo“. Navedlo je, da zahteva, da mora posameznik „dati izjavo“, jasno napotuje na aktivno ravnanje, ne pa na pasivno. Privolitev, dana z vnaprej označenim potrditvenim okencem, pa ne zajema aktivnega ravnanja uporabnika spletnega mesta. Poleg tega je iz zgodovine nastanka člena 5(3) Direktive 2002/58, ki od njegove spremembe z Direktivo 2009/136 določa, da mora uporabnik „dati privolitev“ za namestitev piškotkov, razvidno, da se privolitev uporabnika ne more več predpostavljati in da mora izhajati iz njegovega aktivnega ravnanja. Končno, aktivna privolitev je odslej določena s Splošno uredbo o varstvu podatkov[77], katere člen 4, točka 11, določa, da mora biti izjava volje zlasti v obliki „jasnega pritrdilnega dejanja“, in v katere uvodni izjavi 32 je izrecno izključeno, da gre v primeru „molka, vnaprej označenih okenc ali nedejavnosti“ za privolitev (točke 49, 52, 56 in 62).

Sodišče je zato razsodilo, da privolitev ni veljavna, kadar je shranjevanje informacij ali dostop do informacij, ki so že shranjene v terminalski opremi uporabnika spletnega mesta, dovoljeno na podlagi vnaprej označenega potrditvenega okenca, ki ga mora uporabnik, da zavrne svojo

[73] Ta sodba je bila predstavljena v Letnem poročilu 2019, str. 112 in 113.

[74] Člen 2(f) in člen 5(3) Direktive 2002/58, kakor je bila spremenjena z Direktivo 2009/136/ES Evropskega parlamenta in Sveta z dne 25. novembra 2009 (UL 2009, L 337, str. 11).

[75] Člen 2(h) Direktive 95/46.

[76] Člen 6(1)(a) Uredbe 2016/679.

[77] Člen 6(1)(a) Uredbe 2016/679.

privolitev, odznačiti. Dodalo je, da to, da je uporabnik kliknil na gumb za sodelovanje v zadevni nagradni igri, ne more zadostovati za to, da bi se štelo, da je uporabnik veljavno privolil v namestitev piškotkov (točka 63).

Drugič, Sodišče je ugotovilo, da je namen člena 5(3) Direktive 2002/58 varovati uporabnika pred katerim koli poseganjem v njegovo zasebnost, ne glede na to, ali se to poseganje nanaša na osebne ali druge podatke. Iz tega izhaja, da se pojma „privolitev" ne sme razlagati različno glede na to, ali so informacije, shranjene v terminalski opremi uporabnika spletnega mesta ali iz nje priklicane, osebni podatki ali ne (točki 69 in 71).

Tretjič, Sodišče je navedlo, da člen 5(3) Direktive 2002/58 zahteva, da je uporabnik podal privolitev po tem, ko je bil jasno in izčrpno obveščen med drugim o namenu obdelave. Jasna in izčrpna obvestitev pa mora uporabniku omogočiti, da z lahkoto ugotovi posledice morebitne dane privolitve, in zagotoviti, da je ta privolitev dana ob popolni seznanjenosti z dejstvi. V zvezi s tem je Sodišče štelo, da sta trajanje delovanja piškotkov in možnost oziroma nemožnost tretjih oseb, da dostopajo do teh piškotkov, del jasne in izčrpne obvestitve, ki jo mora ponudnik storitev zagotoviti uporabniku spletnega mesta (točke od 73 do 75 in 81).

VI. Nacionalni nadzorni organi

1. Obseg zahteve po neodvisnosti

Sodba z dne 9. marca 2010 (veliki senat), Komisija/Nemčija (C-518/07, ECLI:EU:C:2010:125)[78]

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.

Zvezna republika Nemčija je trdila, da člen 28(1), drugi pododstavek, Direktive 95/46 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.

Sodišče je razsodilo, da je namen jamstva neodvisnosti nacionalnih nadzornih organov, določenega z Direktivo 95/46, 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

[78] Ta sodba je bila predstavljena v Letnem poročilu 2010, str. 31.

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 in 37 ter 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.

Sodišče je ugotovilo, da Avstrija ni izpolnila obveznosti ter da merila neodvisnosti nadzornega organa iz Direktive 95/46 posledično ne izpolnjuje država članica, ki sprejme ureditev, na katere podlagi je član 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 pomeni, da morajo biti nadzorni organi neodvisni, tako da lahko izvajajo svoje naloge brez zunanjega 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 ni potrebno, da ima nadzorni organ svojo proračunsko rubriko, kakor določa člen 43(3) Uredbe št. 45/2001. Države članice namreč niso zavezane, da v nacionalno zakonodajo vključijo določbe, ki so podobne tistim iz poglavja V Uredbe 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 (točka 58).

Sodba z dne 8. aprila 2014 (veliki senat), Komisija/Madžarska (C-288/12, EU:C:2014:237)[79]

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.

Sodišče je razsodilo, da obveznosti na podlagi Direktive 95/46 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 matični 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).

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

Sodba z dne 1. oktobra 2015, Weltimmo (C-230/14, EU:C:2015:639)[80]

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

[79] Ta sodba je bila predstavljena v Letnem poročilu 2014, str. 57.
[80] Ta sodba je bila predstavljena v Letnem poročilu 2015, str. 49.

neplačanih računov. Po mnenju madžarskega nadzornega organa je družba Weltimmo s tem kršila madžarski zakon, s katerim je bila prenesena Direktiva 95/46.

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. Zato je Sodišču 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 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, 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 nacionalnih nadzornih organov

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

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

Sodišče je v zvezi s tem najprej ugotovilo, da imajo nacionalni nadzorni organi širok razpon pooblastil in da ta pooblastila, netaksativno našteta v členu 28(3) Direktive 95/46, 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 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 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).

Sodba z dne 5. junija 2018 (veliki senat), Wirtschaftsakademie Schleswig-Holstein (C-210/16, ECLI:EU:C:2018:388)

Sodišče se je v tej sodbi (glej tudi razdelek II.5., naslovljen „Pojem ‚upravljavec osebnih podatkov'"), ki se je med drugim nanašala na razlago členov 4 in 28 Direktive 95/46, izreklo o obsegu pooblastil za posredovanje, ki jih imajo nadzorni organi v zvezi z obdelavo osebnih podatkov, ki jo izvaja več akterjev.

Sodišče je tako razsodilo, da lahko nadzorni organ države članice, kadar ima podjetje s sedežem zunaj Evropske unije (kot je ameriška družba Facebook) več poslovnih enot v različnih državah članicah, pooblastila, ki so temu organu podeljena s členom 28(3) te direktive, izvaja v zvezi s poslovno enoto tega podjetja, ki je na ozemlju te države članice (v tem primeru je bila to družba Facebook Germany), čeprav je na podlagi delitve nalog v skupini na eni strani ta poslovna enota zadolžena samo za prodajo oglasnega prostora in druge ukrepe trženja na ozemlju navedene države članice, na drugi strani pa je za zbiranje in obdelavo osebnih podatkov za celotno ozemlje Evropske unije izključno odgovorna poslovna enota, ki je v drugi državi članici (v obravnavanem primeru družba Facebook Ireland) (točka 64 in točka 2 izreka).

Sodišče je poleg tega pojasnilo, da je nadzorni organ države članice, kadar namerava v zvezi s subjektom s sedežem na ozemlju te države članice izvajati pooblastila za posredovanje iz člena 28(3) Direktive 95/46 zaradi kršitev pravil v zvezi z varstvom osebnih podatkov, ki jih je storila tretja oseba, ki je odgovorna za obdelavo teh podatkov in ki ima sedež v drugi državi članici (v obravnavanem primeru družba Facebook Ireland), pristojen za to, da neodvisno od nadzornega organa drugonavedene države članice (Irska) opravi presojo zakonitosti take obdelave podatkov, in lahko svoja pooblastila za posredovanje izvaja v zvezi s subjektom s sedežem na njegovem ozemlju, ne da bi nadzorni organ druge države članice predhodno pozval, naj posreduje (točka 74 in točka 3 izreka).

Sodba z dne 15. junija 2021 (veliki senat), Facebook Ireland in drugi (C-645/19, EU:C:2021:483)

Predsednik Commission belge de la protection de la vie privée (belgijska komisija za varstvo zasebnosti, v nadaljevanju: CPVP) je 11. septembra 2015 pri Nederlandstalige rechtbank van eerste aanleg Brussel (prvostopenjsko sodišče v Bruslju za postopke v nizozemščini, Belgija)

vložil opustitveno tožbo zoper družbe Facebook Ireland, Facebook Inc. in Facebook Belgium, katere namen je bil končati kršitve zakonodaje o varstvu podatkov, ki naj bi jih storila družba Facebook. Te kršitve sta tvorila zlasti zbiranje in uporaba informacij o brskalnih navadah belgijskih uporabnikov interneta, ne glede na to, ali so ti imetniki računa Facebook, z različnimi tehnologijami, kot so piškotki, socialni vtičniki[81] oziroma piksli.

Navedeno sodišče se je 16. februarja 2018 izreklo za pristojno za odločanje o tej tožbi in je meritorno odločilo, da družbeno omrežje Facebook belgijskih uporabnikov interneta ni dovolj obveščalo o zbiranju zadevnih informacij in njihovi uporabi. Poleg tega je bilo ugotovljeno, da privolitev, ki so jo uporabniki interneta dali za zbiranje in obdelavo navedenih informacij, ni veljavna.

Družbe Facebook Ireland, Facebook Inc. in Facebook Belgium so 2. marca 2018 zoper to sodbo vložile pritožbo pri Hof van beroep te Brussel (višje sodišče v Bruslju, Belgija), ki je bilo predložitveno sodišče v obravnavani zadevi. Autorité belge de protection des données (belgijski organ za varstvo podatkov, v nadaljevanju: APD) je pred navedenim sodiščem nastopal kot pravni naslednik predsednika CPVP. Predložitveno sodišče se je izreklo za pristojno za odločanje le o pritožbi, ki jo je vložila družba Facebook Belgium.

Predložitveno sodišče je imelo dvome v zvezi z vplivom uporabe mehanizma „vse na enem mestu“, ki je določen s Splošno uredbo o varstvu podatkov[82], na pristojnosti APD in se je, natančneje, spraševalo, ali lahko APD za dejstva, ki so nastala po začetku veljavnosti Splošne uredbe o varstvu podatkov, torej po 25. maju 2018, vloži tožbo zoper družbo Facebook Belgium, saj je bila kot upravljavec zadevnih podatkov opredeljena družba Facebook Ireland. Od tega datuma in zlasti na podlagi načela „vse na enem mestu“ iz Splošne uredbe o varstvu podatkov naj bi bil namreč za vložitev opustitvene tožbe pristojen le irski pooblaščenec za varstvo podatkov, pod nadzorom irskih sodišč (točki 36 in 37).

Sodišče, ki je odločalo v velikem senatu, je v sodbi pojasnilo, katera so pooblastila nacionalnih nadzornih organov v okviru Splošne uredbe o varstvu podatkov. Tako je zlasti razsodilo, da lahko nadzorni organ države članice na podlagi te uredbe pod nekaterimi pogoji sodišče te države članice opozori na vsakršno domnevno kršitev Splošne uredbe o varstvu podatkov in začne sodni postopek v zvezi s čezmejno obdelavo podatkov,[83] čeprav ni vodilni nadzorni organ glede take obdelave (točka 1 izreka).

Sodišče je na prvem mestu pojasnilo, kateri so pogoji, pod katerimi mora nacionalni nadzorni organ, ki ni vodilni nadzorni organ glede čezmejne obdelave, izvrševati svoje pooblastilo za to, da sodišče države članice opozori na vsakršno domnevno kršitev Splošne uredbe o varstvu podatkov in po potrebi začne sodni postopek, da bi bila zagotovljena uporaba te uredbe. Tako mora biti s Splošno uredbo o varstvu podatkov temu nadzornemu organu po eni strani podeljena pristojnost za sprejemanje odločb o ugotovitvi, da so z navedeno obdelavo kršena

[81] Na primer gumba „všeč mi je“ ali „deli“.

[82] Člen 56(1) Splošne uredbe o varstvu podatkov določa: „Nadzorni organ glavne ali edine ustanovitve [poslovne enote] upravljavca ali obdelovalca je brez poseganja v člen 55 pristojen, da deluje kot vodilni nadzorni organ za obdelavo, ki jo izvaja ta upravljavec ali obdelovalec na čezmejni ravni.“

[83] V smislu člena 4, točka 23, Splošne uredbe o varstvu podatkov.

pravila, ki jih ta uredba vsebuje, po drugi strani pa je treba to pooblastilo izvajati ob spoštovanju postopka sodelovanja in postopka za skladnost iz te uredbe[84] (točka 75 in točka 1 izreka).

Splošna uredba o varstvu podatkov namreč za čezmejne obdelave določa mehanizem „vse na enem mestu“,[85] ki temelji na razdelitvi pristojnosti med „vodilnim nadzornim organom“ in drugimi zadevnimi nacionalnimi nadzornimi organi. Ta mehanizem zahteva tesno, lojalno in učinkovito sodelovanje med temi organi, da se zagotovi dosledna in enotna uporaba pravil o varstvu osebnih podatkov in tako ohrani njihov polni učinek. V Splošni uredbi o varstvu podatkov je v zvezi s tem določena načelna pristojnost vodilnega nadzornega organa za sprejetje odločbe o ugotovitvi, da so s čezmejno obdelavo kršena pravila iz te uredbe,[86] medtem ko je pristojnost drugih nacionalnih nadzornih organov za sprejetje take odločbe, tudi začasne, izjema.[87] Vendar se vodilni nadzorni organ pri izvajanju svojih pristojnosti ne more izogniti nujnemu dialogu ter lojalnemu in učinkovitemu sodelovanju z drugimi zadevnimi nadzornimi organi. Zato vodilni nadzorni organ v okviru tega sodelovanja ne more prezreti stališč drugih zadevnih nadzornih organov, vsak ustrezen in utemeljen ugovor enega od teh organov pa ima učinek vsaj začasne blokade sprejetja osnutka odločitve vodilnega nadzornega organa (točke od 50 do 53, od 56 do 59 in od 63 do 65).

Sodišče je poleg tega pojasnilo, da je okoliščina, da lahko nadzorni organ države članice, ki ni vodilni nadzorni organ glede čezmejne obdelave podatkov, pooblastilo za to, da sodišče države članice opozori na vsakršno domnevno kršitev Splošne uredbe o varstvu podatkov in po potrebi začne sodni postopek, izvršuje le ob upoštevanju pravil o razdelitvi pristojnosti odločanja med vodilnim nadzornim organom in drugimi nadzornimi organi,[88] v skladu s členi 7, 8 in 47 Listine, s katerimi sta zadevni osebi zagotovljeni pravica do varstva njenih osebnih podatkov in pravica do učinkovitega pravnega sredstva (točka 67).

Sodišče je na drugem mestu razsodilo, da izvrševanje pooblastila nadzornega organa države članice, ki ni vodilni nadzorni organ, da začne sodni postopek,[89] v primeru čezmejne obdelave podatkov ne zahteva, da ima upravljavec ali obdelovalec čezmejne obdelave osebnih podatkov, proti kateremu je ta postopek začet, glavno poslovno enoto ali drugo poslovno enoto na ozemlju te države članice. Vendar mora izvrševanje tega pooblastila spadati na ozemeljsko področje uporabe Splošne uredbe o varstvu podatkov,[90] kar pomeni, da mora imeti upravljavec ali obdelovalec čezmejne obdelave poslovno enoto na ozemlju Unije (točke 80, 83 in 84 ter točka 2 izreka).

Sodišče je na tretjem mestu odločilo, da je pooblastilo nadzornega organa države članice, ki ni vodilni nadzorni organ, da sodišče te države članice opozori na vsakršno domnevno kršitev Splošne uredbe o varstvu podatkov in po potrebi začne sodni postopek, v primeru čezmejne obdelave podatkov mogoče izvrševati tako glede glavne poslovne enote upravljavca, ki je v državi

84 Določena v členih 56 in 60 Splošne uredbe o varstvu podatkov.
85 Člen 56(1) Splošne uredbe o varstvu podatkov.
86 Člen 60(7) Splošne uredbe o varstvu podatkov.
87 Člen 56(2) in člen 66 Splošne uredbe o varstvu podatkov določata izjeme od načela pristojnosti vodilnega nadzornega organa za odločanje.
88 Določena v členih 55 in 56 v povezavi s členom 60 Splošne uredbe o varstvu podatkov.
89 V skladu s členom 58(5) Splošne uredbe o varstvu podatkov.
90 Člen 3(1) Splošne uredbe o varstvu podatkov določa, da se ta uredba uporablja za obdelavo osebnih podatkov, ki se izvaja „v okviru dejavnosti ustanovitve [poslovne enote] upravljavca ali obdelovalca v Uniji, ne glede na to, ali obdelava poteka v Uniji ali ne“.

članici tega organa, kot glede druge poslovne enote tega upravljavca, če se sodni postopek nanaša na obdelavo podatkov, ki se izvaja v okviru dejavnosti teh poslovnih enot, in če je navedeni organ pristojen za izvrševanje tega pooblastila.

Vendar je Sodišče pojasnilo, da se za izvrševanje tega pooblastila zahteva, da se Splošna uredba o varstvu podatkov uporablja. Ker so v obravnavani zadevi dejavnosti poslovne enote skupine Facebook v Belgiji neločljivo povezane z obdelavo osebnih podatkov iz postopka v glavni stvari, za katero je na ozemlju Unije odgovorna družba Facebook Ireland, se ta obdelava izvaja „v okviru dejavnosti ustanovitve [poslovne enote] upravljavca“ in torej spada na področje uporabe Splošne uredbe o varstvu podatkov (točke od 94 do 96 ter točka 3 izreka).

Sodišče je na četrtem mestu razsodilo, da kadar je nadzorni organ države članice, ki ni „vodilni nadzorni organ“, sodni postopek v zvezi s čezmejno obdelavo osebnih podatkov začel pred začetkom veljavnosti Splošne uredbe o varstvu podatkov, je ta postopek z vidika prava Unije mogoče nadaljevati na podlagi določb Direktive 95/46, ki se še naprej uporablja za kršitve pravil iz te direktive, ki so bile storjene do datuma njene razveljavitve. Poleg tega lahko ta organ ta postopek začne zaradi kršitev, ki so bile storjene po datumu začetka veljavnosti Splošne uredbe o varstvu podatkov, če gre za enega od primerov, v katerih je s to uredbo navedenemu organu izjemoma podeljena pristojnost za sprejetje odločbe o ugotovitvi, da so z zadevno obdelavo podatkov kršena pravila iz te uredbe, ter ob spoštovanju postopka sodelovanja in postopka za skladnost, določenih v tej uredbi (točka 105 in točka 4 izreka).

Sodišče je na petem in zadnjem mestu priznalo neposredni učinek določbe Splošne uredbe o varstvu podatkov, v skladu s katero vsaka država članica z zakonom določi, da ima njen nadzorni organ pooblastila, da sodišča opozori na kršitve te uredbe in po potrebi začne sodne postopke. Zato se tak organ na to določbo lahko sklicuje, da bi začel ali nadaljeval postopek proti posameznikom, tudi če ta določba ni bila posebej prenesena v zakonodajo zadevne države članice (točka 113 in točka 5 izreka).

VII. 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 V.1., naslovljen „Pravica do ugovora zoper obdelavo osebnih podatkov (‚pravica biti pozabljen‘)“) odločilo tudi o ozemeljskem področju uporabe Direktive 95/46.

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, 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).

VIII. 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) so morale britanske pivovarne poslovodjem 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 ni spadala 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 št. 45/2001.

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 št. 1049/2001[91] o dostopu do dokumentov pridobiti dostop do dokumentov, ki vsebujejo osebne podatke, postanejo določbe Uredbe 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 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 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 poseglo v zakonite interese posameznikov, na katere se nanašajo osebni podatki, kot določa člen 8(b) Uredbe št. 45/2001 (točka 78).[92]

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,[93] v skladu s katerim vlagatelj zahtevka za registracijo dajanja fitofarmacevtskih 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 št. 45/2001, skrila imena teh strokovnjakov. V zvezi s tem je navedla, da razkritje imen teh

[91] 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).

[92] Ta sodba je bila predstavljena v Letnem poročilu 2010, str. 14.

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

strokovnjakov ustreza prenosu osebnih podatkov v smislu člena 8 Uredbe 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 sodbo[94] 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 št. 45/2001. Ker pojma „osebni podatek" v smislu člena 2(a) Uredbe 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 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, 1.04.03.10, 1.04.03.11, 2.04, 2.05.00, 4.11.01, 4.11.07 in 4.11.11.01.

---

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