SODIŠČE
EVROPSKE UNIJE

SL

Tematski prikaz
Varstvo osebnih podatkov

Direktorat za raziskave in dokumentacijo

curia.europa.eu

Predgovor

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

Določena je v primarnem pravu, zlasti v členu 8 Listine Evropske unije o temeljnih pravicah (v nadaljevanju: Listina) in členu 16(1) Pogodbe o delovanju Evropske unije (PDEU). Ta temeljna pravica je tesno povezana s pravico do spoštovanja zasebnega življenja iz člena 7 Listine.

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 razveljavljena leta 2018, je bila v tem pogledu osrednji pravni akt Unije na tem področju.

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] Navesti je treba, da je zakonodajalec Unije zaradi upoštevanja tehnološkega in tržnega razvoja leta 2017 začel ponovni pregled te direktive,[4] ki še vedno poteka.[5]

Evropska unija je leta 2016 prenovila celoten pravni okvir na tem področju. Za to je sprejela Uredbo (EU) 2016/679[6] o varstvu osebnih podatkov (v nadaljevanju: SUVP), 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, katere določbe se uporabljajo od 6. maja 2018.

---

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, razveljavljena s 25. majem 2018 (glej opombo 6).

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 v sodbi z dne 8. aprila 2014, Digital Rights Ireland in Seitlinger in drugi (C-293/12 in C-594/12, *EU:C:2014:238*), to direktivo razveljavilo, ker je resno posegala v pravico do spoštovanja zasebnega življenja in varstva osebnih podatkov (glej oddelek I.1., naslovljen „Skladnost sekundarnega prava Unije s pravico do varstva osebnih podatkov“ tega dokumenta).

4 Komisija je 10. januarja 2017 predstavila predlog za nadomestitev te direktive z uredbo o zasebnosti in elektronskih komunikacijah.

5 Svet Evropske unije je 10. februarja 2021 odobril pogajalski mandat za revizijo pravil o varstvu zasebnosti in zaupnosti pri uporabi elektronskih komunikacijskih storitev, kar je omogočilo začetek pogajanj z Evropskim parlamentom. Besedilo predloga uredbe Evropskega parlamenta in Sveta o spoštovanju zasebnosti in varstvu osebnih podatkov na področju elektronskih komunikacij ter razveljavitvi Direktive 2002/58/ES (uredba o zasebnosti in elektronskih komunikacijah) je dostopno na: *https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_6087_2021_INIT&from=EN*).

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).

Kar zadeva obdelavo osebnih podatkov v institucijah in organih EU, je varstvo teh podatkov od 11. decembra 2018 zagotovljeno zlasti z Uredbo (EU) 2018/1725[8]. Za zagotovitev usklajenega pristopa k varstvu osebnih podatkov po vsej Uniji se s to uredbo pravila na tem področju čim bolj usklajujejo z ureditvijo, ki je bila uvedena s SUVP.

Nazadnje, zakonodajalec Unije je za soočanje z izzivi, ki jih prinašajo nove tehnologije, od leta 2020 začel sprejemati nove zakonodajne ukrepe[9], ki so povezani z določbami prava Unije o varstvu osebnih podatkov.

Glede na obsežno sodno prakso Sodišča na področju varstva osebnih podatkov je namen tega tematskega prikaza predstaviti izbor temeljnih sodb s tega področja in sodb, ki so pomembno prispevale k razvoju te sodne prakse, s posebnim poudarkom na sodbah, ki jih je izdal veliki senat Sodišča. Natančneje, cilj tega dokumenta je zajeti sodno prakso v zvezi s splošnimi predpisi o varstvu osebnih podatkov, ki izhajajo iz razlage Direktive 95/46 in SUVP, ter sodno prakso v zvezi s sektorskimi predpisi, zlasti na področju elektronskih komunikacij in kazenskega prava. Poleg tega se želi z njim predstaviti izbor sodb, ki se nanašajo na predpise, ki se uporabljajo transverzalno, hkrati pa že na začetku poudariti odločilno vlogo Listine pri razvoju sodne prakse.

8 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 (UL 2018, L 295, str. 39).

9 V tem okviru je treba zlasti omeniti tri zakonodajne pobude: (i) Uredba (EU) 2022/868 Evropskega parlamenta in Sveta z dne 30. maja 2022 o evropskem upravljanju podatkov in spremembi Uredbe (EU) 2018/1724 (Akt o upravljanju podatkov) (UL 2022, L 152, str. 1) in Uredba (EU) 2023/2854 Evropskega parlamenta in Sveta z dne 13. decembra 2023 o harmoniziranih pravilih za pravičen dostop do podatkov in njihovo uporabo ter spremembi Uredbe (EU) 2017/2394 in Direktive (EU) 2020/1828 (Akt o podatkih) (UL 2023, L 2854, str. 1); (ii) sveženj zakonodajnih aktov o digitalnih storitvah in trgih, ki ga sestavljata Uredba (EU) 2022/2065 Evropskega parlamenta in Sveta z dne 19. oktobra 2022 o enotnem trgu digitalnih storitev in spremembi Direktive 2000/31/ES (Akt o digitalnih storitvah) (UL 2022, L 277, str. 1) in Uredba (EU) 2022/1925 Evropskega parlamenta in Sveta z dne 14. septembra 2022 o tekmovalnih in pravičnih trgih v digitalnem sektorju ter spremembi direktiv (EU) 2019/1937 in (EU) 2020/1828 (Akt o digitalnih trgih) (UL 2022, L 265, str. 1), in (iii) prvi zakonodajni predlog za oblikovanje regulativnega okvira na področju umetne inteligence, ki je bil sprejet z Aktom o umetni inteligenci (UL 2024, L 1689).

Kazalo

PREDGOVOR 4
I. PRAVICA DO VARSTVA OSEBNIH PODATKOV, PRIZNANA Z LISTINO EVROPSKE UNIJE O TEMELJNIH PRAVICAH 7
1. Skladnost sekundarnega prava Unije s pravico do varstva osebnih podatkov 7
2. Spoštovanje pravice do varstva osebnih podatkov pri izvajanju prava Unije 17
II. OBDELAVA OSEBNIH PODATKOV V SMISLU SPLOŠNE UREDITVE S TEGA PODROČJA 19
1. Področje uporabe splošne ureditve 19
2. Pojem „osebni podatki“ 24
3. Pojem „obdelava osebnih podatkov“ 26
4. Pojem „zbirka osebnih podatkov“ 30
5. Pojem „upravljavec osebnih podatkov“ 31
6. Pojem „skupni upravljavec“ 33
7. Pogoji zakonitosti obdelave osebnih podatkov 33
III. OBDELAVA OSEBNIH PODATKOV V SMISLU SEKTORSKIH PREDPISOV 39
1. Obdelava osebnih podatkov na področju elektronskih komunikacij 39
2. Obdelava osebnih podatkov v kazenskih zadevah 56
IV. PRENOS OSEBNIH PODATKOV V TRETJE DRŽAVE 60
V. VARSTVO OSEBNIH PODATKOV NA INTERNETU 67
1. Pravica do ugovora zoper obdelavo osebnih podatkov („pravica biti pozabljen“) 67
2. Obdelava osebnih podatkov in pravice intelektualne lastnine 68
3. Odstranitev povezav do osebnih podatkov 71
4. Privolitev uporabnika spletnega mesta v shranjevanje informacij 79
5. Obdelava osebnih podatkov na spletnih družbenih omrežjih 80
VI. NACIONALNI NADZORNI ORGANI 84
1. Obseg zahteve po neodvisnosti 84
2. Določitev prava, ki se uporablja, in pristojnega nadzornega organa 86
3. Pooblastila nacionalnih nadzornih organov 87
4. Pogoji za naložitev upravnih glob 92
5. Povezava pristojnosti nacionalnih nadzornih organov s pristojnostmi drugih nacionalnih organov 95

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)

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[10] in 259/2008[11], 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.

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. Sodišče je v tem okviru menilo, da imajo davkoplačevalci v demokratični družbi sicer pravico biti

[10] Uredba Sveta (ES) št. 1290/2005 z dne 21. junija 2005 o financiranju skupne kmetijske politike (UL 2005, L 209, str. 1), 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).

[11] Uredba Komisije (ES) št. 259/2008 z dne 18. marca 2008 o podrobnih pravilih za uporabo Uredbe Sveta (ES) št. 1290/2005 glede objavljanja informacij o upravičencih do sredstev iz EKJS in 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).

obveščeni o uporabi javnih sredstev, vendar bi morala Svet in Komisija uravnotežiti različne zadevne interese, kar pomeni, da bi morala pred sprejetjem spornih določb preveriti, ali to, da država članica objavi te podatke na enem samem spletnem mestu, ne presega tistega, kar je potrebno za uresničitev legitimnih ciljev, ki se jim sledi.

Tako je Sodišče ugotovilo, da so nekatere določbe Uredbe št. 1290/2005 in vse določbe Uredbe št. 259/2008 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. 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.

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)

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-293/12 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 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.

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. 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. 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. 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.

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.

Sodba z dne 21. junija 2022 (veliki senat), Ligue des droits humains (C-817/19, EU:C:2022:491)

Podatki PNR (Passenger Name Record) so informacije o rezervaciji, ki jih letalski prevozniki hranijo v svojih sistemih rezervacij in sistemih za nadzor odhodov. V skladu z

Direktivo o PNR[12] morajo ti prevozniki zaradi boja proti terorizmu in hudim kaznivim dejanjem posredovati podatke o vsakem potniku na letu zunaj EU, ki je opravljen med tretjo državo in Evropsko unijo, enoti za informacije o potnikih namembne države članice ali države članice odhoda zadevnega leta. Tako posredovani podatki PNR so namreč predmet predhodnega ocenjevanja enote za informacije o potnikih[13] in se nato hranijo za morebitno naknadno ocenjevanje, ki ga opravijo pristojni organi zadevne države članice ali pristojni organi druge države članice. Države članice se lahko odločijo, da bodo direktivo uporabljale tudi za lete znotraj EU[14].

Ligue des droits humains je pri Cour constitutionnelle (ustavno sodišče, Belgija) vložilo ničnostno tožbo zoper belgijski zakon, s katerim sta bili v nacionalno pravo preneseni Direktiva o PNR in Direktiva o API[15]. Tožeča stranka je menila, da se s tem zakonom krši pravica do zasebnosti in varstva osebnih podatkov. Na eni strani je tožeča stranka grajala obsežnost podatkov PNR, na drugi strani pa splošnost zbiranja, prenosa in obdelave teh podatkov. Ta zakon naj bi posegal tudi v prosto gibanje oseb, ker naj bi s tem, da sistem PNR razširja na lete znotraj Unije ter na prevoze, opravljene z drugimi prevoznimi sredstvi znotraj Unije, posredno ponovno vzpostavil mejne kontrole.

V teh okoliščinah je belgijsko ustavno sodišče Sodišču postavilo vprašanja za predhodno odločanje, ki se med drugim nanašajo na veljavnost Direktive o PNR.

Sodišče je s sodbo, izdano v velikem senatu, potrdilo veljavnost Direktive o PNR v delu, v katerem jo je mogoče razlagati v skladu z Listino.

V zvezi s tem je Sodišče odločilo, da razlaga Sodišča glede določb Direktive o PNR ob upoštevanju temeljnih pravic, zagotovljenih s členi 7, 8 in 21 ter členom 52(1) Listine[16], zagotavlja skladnost te direktive s temi členi, zato pri preučitvi postavljenih vprašanj ni bil ugotovljen noben element, ki bi lahko vplival na veljavnost navedene direktive.

Sodišče je najprej opozorilo, da se akt Unije, kolikor je le mogoče, razlaga tako, da se ne vzbuja dvom o njegovi veljavnosti, in v skladu z vsem primarnim pravom ter predvsem z določbami Listine, zato morajo države članice paziti, da se ne oprejo na tako razlago tega akta, ki bi bila v nasprotju s temeljnimi pravicami, ki jih varuje pravni red Unije, ali z drugimi splošnimi načeli pravnega reda Unije. Sodišče je v zvezi z Direktivo o PNR

---

12 Direktiva (EU) 2016/681 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o uporabi podatkov iz evidence podatkov o potnikih (PNR) za preprečevanje, odkrivanje, preiskovanje in pregon terorističnih in hudih kaznivih dejanj (UL 2016, L 119, str. 132) (v nadaljevanju: Direktiva o PNR).

13 Namen tega predhodnega ocenjevanja je identifikacija oseb, ki jih morajo pristojni organi podrobneje preveriti, glede na dejstvo, da bi lahko sodelovale pri terorističnem ali hudem kaznivem dejanju. To predhodno ocenjevanje se izvaja sistematično in z avtomatiziranimi sredstvi tako, da se podatki PNR primerjajo s podatkovnimi zbirkami, ki so „pomembne“, ali da se obdelujejo glede na vnaprej določena merila iz člena 6(2)(a) in (3) Direktive o PNR.

14 Ob uporabi možnosti, določene v členu 2 Direktive o PNR.

15 Direktiva Sveta 2004/82/ES z dne 29. aprila 2004 o dolžnosti prevoznikov, da posredujejo podatke o potnikih (UL, posebna izdaja v slovenščini, poglavje 19, zvezek 7, str. 74; v nadaljevanju: Direktiva o API). Ta direktiva ureja posredovanje predhodnih informacij o potnikih (kot so številka in vrsta uporabljene potne listine ter državljanstvo) letalskih prevoznikov pristojnim nacionalnim organom zaradi izboljšanja mejne kontrole in boja proti nezakonitemu priseljevanju.

16 V skladu s to določbo mora biti kakršno koli omejevanje uresničevanja pravic in svoboščin, ki jih priznava ta listina, predpisano z zakonom in spoštovati bistveno vsebino teh pravic in svoboščin. Poleg tega so omejitve teh pravic in svoboščin dovoljene samo, če so potrebne in če dejansko ustrezajo ciljem splošnega interesa, ki jih priznava Unija, ali če so potrebne zaradi zaščite pravic in svoboščin drugih.

pojasnilo, da se z mnogimi uvodnimi izjavami in določbami te direktive zahteva taka skladna razlaga, pri čemer je poudarjen pomen, ki ga zakonodajalec Unije s sklicevanjem na visoko raven varstva podatkov pripisuje popolnemu spoštovanju temeljnih pravic, določenih v Listini.

Sodišče je ugotovilo, da Direktiva o PNR vsebuje nedvomno resna poseganja v pravice, zagotovljene s členoma 7 in 8 Listine, med drugim ker je namen te direktive vzpostaviti sistem stalnega, neciljnega in sistematičnega nadzora, ki vključuje avtomatizirano ocenjevanje osebnih podatkov vseh oseb, ki uporabljajo storitve letalskega prevoza. Sodišče je spomnilo, da je treba možnost držav članic, da upravičijo takšno poseganje, presojati tako, da se oceni teža poseganja in preveri, ali je pomembnost cilja v splošnem interesu, ki se uresničuje, v sorazmerju s to težo.

Sodišče je ugotovilo, da se lahko šteje, da so prenos, obdelava in hramba podatkov PNR, ki jih določa ta direktiva, omejeni na tisto, kar je nujno potrebno za namene boja proti terorističnim in hudim kaznivim dejanjem, če se pooblastila, določena s to direktivo, razlagajo ozko. V zvezi s tem je v izdani sodbi med drugim določeno:

- Sistem, vzpostavljen z Direktivo o PNR, lahko zajema le jasno opredeljive in omejene informacije iz rubrik Priloge I k tej direktivi, ki so povezane z opravljenim letom in zadevnim potnikom, kar za nekatere rubrike iz te priloge pomeni, da so zajete le informacije, na katere se te rubrike izrecno sklicujejo.[17]
- Uporaba sistema, vzpostavljenega z Direktivo o PNR, mora biti omejena na teroristična kazniva dejanja in samo na huda kazniva dejanja, ki so objektivno, vsaj posredno, povezana z letalskim prevozom potnikov. V zvezi s temi hudimi kaznivimi dejanji je treba navesti, da uporabe tega sistema ni mogoče razširiti na kazniva dejanja, ki – čeprav izpolnjujejo merilo iz te direktive v zvezi s pragom teže in so med drugim navedena v Prilogi II k tej direktivi – ob upoštevanju posebnosti nacionalnega kazenskega sistema spadajo med splošna kazniva dejanja.
- Morebitna razširitev uporabe Direktive o PNR na vse ali del letov znotraj EU, za katero se lahko država članica odloči tako, da uporabi možnost, določeno s to direktivo, mora biti omejena na tisto, kar je nujno potrebno. Za to mora biti mogoče, da je ta razširitev predmet učinkovitega nadzora sodišča ali neodvisnega upravnega organa, katerega odločitev je zavezujoča. V zvezi s tem je Sodišče pojasnilo:
  - Le v položaju, v katerem navedena država članica ugotovi, da obstajajo dovolj konkretne okoliščine, zaradi katerih je mogoče šteti, da se ta država članica spopada s terorističnо grožnjo, ki se izkaže za resnično in sedanjo ali predvidljivo, uporaba te direktive za vse lete znotraj EU, ki prihajajo iz

[17] Tako morajo biti zlasti „podatki o načinu plačila“ (rubrika 6 Priloge) omejeni na način plačila in izstavitev računa za letalsko vozovnico, pri čemer so izvzeti kakršni koli drugi podatki, ki niso neposredno povezani z letom, „splošne opombe“ (rubrika 12) pa se lahko nanašajo le na informacije, ki so izrecno naštete v tej rubriki in ki se nanašajo na mladoletne potnike.

navedene države članice ali so vanjo namenjeni, za obdobje, časovno omejeno na tisto, kar je nujno potrebno, vendar ga je mogoče podaljšati, ne presega meja tega, kar je nujno potrebno.[18]

- Ob neobstoju takšne teroristične grožnje uporabe navedene direktive ni mogoče razširiti na vse lete znotraj EU, ampak mora biti omejena na lete znotraj EU, ki se med drugim nanašajo na nekatere letalske povezave, določene potovalne načrte ali celo na nekatera letališča, za katera po presoji zadevne države članice obstajajo indici, ki lahko upravičijo to uporabo. To, da je ta uporaba za lete znotraj EU, ki so tako izbrani, nujno potrebna, je treba redno pregledovati glede na razvoj okoliščin, ki so utemeljevale njihovo izbiro.

- Enota za informacije o potnikih lahko pri predhodnem ocenjevanju podatkov PNR, katerega namen je identificirati osebe, ki jih je treba podrobneje preveriti pred njihovim prihodom oziroma odhodom, in ki se najprej opravi z avtomatiziranimi obdelavami, po eni strani primerja te podatke zgolj s podatkovnimi zbirkami o osebah ali predmetih, ki so iskani ali so zanje razpisani ukrepi.[19] Te podatkovne zbirke morajo biti nediskriminatorne, uporabljajo pa jih lahko pristojni organi v povezavi z bojem proti terorističnim in hudim kaznivim dejanjem, ki so objektivno, vsaj posredno, povezana z letalskim prevozom potnikov. Po drugi strani enota za informacije o potnikih v zvezi s predhodnim ocenjevanjem glede na vnaprej določena merila ne sme uporabljati tehnologij umetne inteligence v okviru sistemov samostojnega učenja („machine learning“), ki lahko brez človekovega posredovanja in nadzora spremenijo postopek ocenjevanja ter zlasti merila za ocenjevanje, na katerih temelji rezultat uporabe tega postopka, in težo teh meril. Navedena merila morajo biti določena tako, da je njihova uporaba usmerjena izrecno na posameznike, glede katerih bi lahko obstajal utemeljen sum sodelovanja pri terorističnih ali hudih kaznivih dejanjih, in da se upoštevajo tako „obremenilni“ kot „razbremenilni“ dokazi, ne da bi povzročala neposredno ali posredno diskriminacijo.[20]

- Glede na stopnjo napake, ki je neločljivo povezana s tako avtomatizirano obdelavo podatkov PNR, in glede na precejšnje število „lažno pozitivnih“ rezultatov, pridobljenih na podlagi teh avtomatiziranih obdelav v letih 2018 in 2019, je primernost sistema, vzpostavljenega z Direktivo o PNR, za uresničevanje ciljev, ki se jim sledi, odvisna predvsem od pravilnega delovanja

---

18 Zaradi obstoja take grožnje same po sebi se namreč lahko vzpostavi povezava med prenosom in obdelavo zadevnih podatkov ter bojem proti terorizmu. Zato določitev uporabe Direktive o PNR za vse lete znotraj EU, ki prihajajo iz zadevne države članice ali so vanjo namenjeni, za omejeno obdobje ne presega meja tega, kar je nujno potrebno, pri čemer mora biti mogoče, da je odločba, ki določa to uporabo, predmet nadzora sodišča ali neodvisnega upravnega organa.

19 To so podatkovne zbirke o osebah ali predmetih, ki so iskani ali so zanje razpisani ukrepi v smislu člena 6(3)(a) Direktive o PNR. Analize na podlagi različnih podatkovnih zbirk pa bi lahko bile v obliki podatkovnega rudarjenja („data mining“) in bi lahko povzročile nesorazmerno uporabo teh podatkov, ki bi omogočala ugotovitev natančnega profila zadevnih oseb zgolj zato, ker te osebe nameravajo potovati z letalom.

20 Vnaprej določena merila morajo biti ciljna, sorazmerna in specifična ter jih je treba redno pregledovati (člen 6(4) Direktive o PNR). Predhodno ocenjevanje glede na vnaprej določena merila se mora izvajati na nediskriminatoren način. V skladu s členom 6(4), četrti stavek, Direktive o PNR ta merila nikakor ne smejo temeljiti na rasi ali etničnem poreklu osebe, njenih političnih mnenjih, veri ali filozofskem prepričanju, članstvu v sindikatu, zdravstvenem stanju, spolnem življenju ali spolni usmerjenosti.

preverjanja pozitivnih rezultatov, pridobljenih na podlagi teh obdelav, ki ga enota za informacije o potnikih nato opravi z neavtomatiziranimi sredstvi. Države članice morajo v zvezi s tem določiti jasna in natančna pravila, na podlagi katerih se lahko usmerja in omeji analiza, ki jo opravijo uslužbenci enote za informacije o potnikih, odgovorni za posamičen pregled, da se zagotovi popolno spoštovanje temeljnih pravic, določenih v členih 7, 8 in 21 Listine, ter zlasti skladna upravna praksa znotraj enote za informacije o potnikih, s katero se upošteva načelo prepovedi diskriminacije. Natančneje, države članice se morajo prepričati, da enota za informacije o potnikih jasno in natančno določi objektivna merila za pregled, na podlagi katerih lahko njeni uslužbenci preverijo, prvič, ali in kako se določen zadetek („hit“) dejansko nanaša na posameznika, ki bi lahko sodeloval pri terorističnih ali hudih kaznivih dejanjih, in drugič, nediskriminatorno naravo avtomatiziranih obdelav. V tem okviru je Sodišče še poudarilo, da se morajo pristojni organi prepričati, da zadevna oseba lahko razume, kako vnaprej določena merila za ocenjevanje in programi, pri katerih se ta merila uporabljajo, delujejo, tako da se lahko ta oseba ob popolnem poznavanju zadeve odloči, ali bo uveljavljala svojo pravico do sodnega varstva. Prav tako morata imeti v okviru pravnega sredstva sodišče, pristojno za nadzor nad zakonitostjo odločitve, ki so jo sprejeli pristojni organi, in – razen v primeru groženj državni varnosti – zadevna oseba možnost, da se seznanita z vsemi razlogi in dokazi, na podlagi katerih je bila ta odločitev sprejeta, vključno z vnaprej določenimi merili za ocenjevanje in delovanje programov, pri katerih se ta merila uporabljajo.

– Naknadno zagotavljanje in naknadno ocenjevanje podatkov PNR, torej po prihodu ali odhodu zadevne osebe, je mogoče opraviti zgolj na podlagi novih okoliščin in objektivnih elementov, na podlagi katerih je mogoče utemeljiti utemeljen sum sodelovanja te osebe pri hudih kaznivih dejanjih, ki so objektivno, vsaj posredno, povezana z letalskim prevozom potnikov, ali šteti, da bi ti podatki v konkretnem primeru učinkovito prispevali k boju proti terorističnim kaznivim dejanjem s takšno povezavo. Za zagotavljanje podatkov PNR za namene takšnega naknadnega ocenjevanja načeloma, razen v nujnih primerih, ki so ustrezno utemeljeni, sodišče ali neodvisen upravni organ opravi predhodni nadzor na podlagi obrazloženega zaprosila pristojnih organov, in to ne glede na to, ali je to zaprosilo vloženo pred iztekom šestmesečnega obdobja od prenosa teh podatkov enoti za informacije o potnikih ali pa se vloži po izteku tega obdobja.[21]

[21] V skladu s členom 12(1) in (3) Direktive o PNR je tak nadzor izrecno določen le za zaprosila za razkritje podatkov PNR, vložena po izteku šestmesečnega obdobja od prenosa teh podatkov enoti za informacije o potnikih.

Sodba z dne 22. novembra 2022 (veliki senat), Luxembourg Business Registers (C-37/20 in C-601/20, EU:C:2022:912)

Z namenom boja proti pranju denarja in financiranju terorizma Direktiva o preprečevanju pranja denarja[22] državam članicam nalaga, naj vodijo register, ki vsebuje podatke o dejanskih lastnikih[23] gospodarskih in drugih pravnih subjektov, ustanovljenih na njihovem ozemlju. Po spremembi te direktive z Direktivo 2018/843[24] morajo imeti do nekaterih od teh informacij vedno dostop vsi člani širše javnosti. V skladu s tako spremenjeno Direktivo o preprečevanju pranja denarja (v nadaljevanju: spremenjena Direktiva o preprečevanju pranja denarja) je bil z luksemburško zakonodajo ustanovljen register dejanskih lastnikov (v nadaljevanju: RDL), namenjen hrambi in dajanju na voljo vrste informacij o dejanskih lastnikih registriranih subjektov, do katerih ima dostop vsakdo.

V teh okoliščinah sta bili pri Tribunal d'arrondissement de Luxembourg (okrožno sodišče v Luxembourgu) predloženi dve zadevi, ki sta ju vložili oseba WM in družba Sovim SA, ki izpodbijata odločbi združenja Luxembourg Business Registers, upravljavca sistema RDL, s katerima je to zavrnilo njuni prošnji za preprečitev dostopa širše javnosti do informacij, ki se v prvi zadevi nanašajo na osebo WM, dejansko lastnico nepremičninske družbe, v drugi zadevi pa na dejanskega lastnika družbe Sovim SA. V okviru teh dveh zadev je Tribunal d'arrondissement de Luxembourg (okrožno sodišče v Luxembourgu) Sodišču predložilo vprašanje za predhodno odločanje v zvezi z veljavnostjo določb prava Unije, s katerimi je bil vzpostavljen sistem dostopa javnosti do informacij o dejanskih lastnikih, o kateri je dvomilo.

Sodišče, ki je zasedalo v velikem senatu, je Direktivo 2018/843 razglasilo za neveljavno v delu, v katerem je bila z njo Direktiva o preprečevanju pranja denarja spremenjena tako, da morajo države članice zagotoviti, da imajo do informacij o dejanskih lastnikih gospodarskih in drugih pravnih subjektov, ustanovljenih na njihovem ozemlju, vedno dostop vsi člani širše javnosti.[25]

Na prvem mestu, Sodišče je ugotovilo, da dostop širše javnosti do informacij o dejanskih lastnikih, določen s spremenjeno Direktivo o preprečevanju pranja denarja, pomeni resno poseganje v temeljni pravici do spoštovanja zasebnega življenja in do varstva osebnih podatkov, določeni v členih 7 in 8 Listine.

V zvezi s tem je Sodišče ugotovilo, da ker zadevni podatki vsebujejo informacije o določenih fizičnih osebah, in sicer o dejanskih lastnikih gospodarskih in drugih pravnih

---

22 Direktiva (EU) 2015/849 Evropskega parlamenta in Sveta z dne 20. maja 2015 o preprečevanju uporabe finančnega sistema za pranje denarja ali financiranje terorizma, spremembi Uredbe (EU) št. 648/2012 Evropskega parlamenta in Sveta ter razveljavitvi Direktive 2005/60/ES Evropskega parlamenta in Sveta in Direktive Komisije 2006/70/ES (UL 2015, L 141, str. 73, v nadaljevanju: Direktiva o preprečevanju pranja denarja).

23 V skladu s členom 3, točka 6, Direktive o preprečevanju pranja denarja dejanski lastnik pomeni fizične osebe, ki končno posedujejo ali nadzirajo stranko in/ali fizično osebo oziroma osebe, v imenu katerih se izvaja transakcija ali opravlja dejavnost.

24 Direktiva (EU) 2018/843 Evropskega parlamenta in Sveta z dne 30. maja 2018 o spremembi Direktive (EU) 2015/849 o preprečevanju uporabe finančnega sistema za pranje denarja ali financiranje terorizma ter o spremembi direktiv 2009/138/ES in 2013/36/EU (UL 2018, L 156, str. 43).

25 Neveljavnost člena 1, točka 15(c), Direktive (EU) 2018/843 o spremembi člena 30(5), prvi pododstavek, točka (c), Direktive o preprečevanju pranja denarja.

subjektov, ustanovljenih na ozemlju držav članic, dostop vseh članov širše javnosti do njih posega v temeljno pravico do spoštovanja zasebnega življenja. Poleg tega to, da se dostop do teh informacij zagotovi splošni javnosti, pomeni obdelavo osebnih podatkov. Dodalo je, da tako zagotavljanje dostopa splošni javnosti pomeni poseganje v zgoraj navedeni temeljni pravici, ne glede na nadaljnjo uporabo sporočenih informacij.

V zvezi z resnostjo tega poseganja je Sodišče navedlo, da ker se informacije, dostop do katerih je omogočen širši javnosti, nanašajo na identiteto dejanskega lastnika ter na naravo in obseg deležev, ki jih ta ima v gospodarskih ali drugih pravnih subjektih, lahko te informacije omogočijo oblikovanje profila, ki vsebuje nekatere osebne identifikacijske podatke, premoženjsko stanje zadevne osebe ter specifične gospodarske sektorje, države in podjetja, v katere je investirala. Poleg tega te informacije postanejo dostopne potencialno neomejenemu številu oseb, tako da lahko taka obdelava osebnih podatkov omogoči tudi osebam, ki se želijo iz razlogov, nepovezanih s ciljem, ki mu sledi ta ukrep, seznaniti zlasti s premoženjskim in finančnim položajem dejanskega lastnika, da do navedenih informacij prosto dostopajo. Ta možnost je še toliko bolj olajšana, kadar si je mogoče zadevne podatke ogledati na spletu. Poleg tega potencialne posledice za zadevne osebe, ki jih povzroči morebitna zloraba njihovih osebnih podatkov, še zaostruje to, da si je mogoče te podatke po tem, ko je bil dostop do njih omogočen širši javnosti, ne le prosto ogledati, ampak jih tudi shraniti in razširjati, in da je tako tem osebam še toliko težje ali celo iluzorno, da bi se učinkovito branile pred zlorabami.

Na drugem mestu, Sodišče je v okviru preizkusa upravičenosti zadevnega posega, prvič, ugotovilo, da je v obravnavani zadevi spoštovano načelo zakonitosti. Omejitev uresničevanja zgoraj navedenih temeljnih pravic, ki je posledica dostopa širše javnosti do informacij o dejanskih lastnikih, je namreč določena z zakonodajnim aktom, in sicer s spremenjeno Direktivo o preprečevanju pranja denarja. Poleg tega ta direktiva na eni strani določa, da morajo biti te informacije ustrezne, natančne in aktualne, pri čemer so v njej so izrecno našteti nekateri podatki, do katerih je treba omogočiti dostop javnosti. Po drugi strani določa pogoje, pod katerimi lahko države članice določijo izjeme od takega dostopa.

Drugič, Sodišče je pojasnilo, da zadevno poseganje ne posega v bistveno vsebino temeljnih pravic, določenih v členih 7 in 8 Listine. Čeprav je res, da spremenjena Direktiva o preprečevanju pranja denarja ne vsebuje izčrpnega seznama podatkov, dostop do katerih mora biti omogočen vsem članom širše javnosti, in da države članice lahko zagotavljajo dostop do dodatnih informacij, pa je mogoče pridobiti in imeti na voljo ter s tem potencialno narediti dostopne javnosti zgolj ustrezne informacije o dejanskih lastnikih in deležih, ki jih imajo ti v lasti, s čimer so zlasti izključene informacije, ki niso v ustrezni zvezi s cilji spremenjene Direktive o preprečevanju pranja denarja. Ni pa očitno, da bi omogočanje dostopa širši javnosti do informacij, ki so v taki zvezi, kakor koli oslabila bistveno vsebino zadevnih temeljnih pravic.

Tretjič, Sodišče je poudarilo, da je zakonodajalec Unije s tem, da je določil dostop širše javnosti do informacij o dejanskih lastnikih, želel preprečiti pranje denarja in financiranje

terorizma, saj bi bilo zaradi večje transparentnosti vzpostavljeno okolje, ki je manj primerno za uresničevanje teh namenov, kar je cilj splošnega interesa, s katerim je mogoče upravičiti poseganja, tudi resna, v temeljne pravice, določene v členih 7 in 8 Listine.

Četrtič, Sodišče je v okviru preizkusa primernosti, nujnosti in sorazmernosti zadevnega poseganja ugotovilo, da je dostop širše javnosti do informacij o dejanskih lastnikih gotovo primeren za to, da prispeva k uresničitvi tega cilja.

Vendar meni, da za to poseganje ni mogoče šteti, da je omejeno na to, kar je nujno potrebno. Na eni strani nujne potrebe za navedeno poseganje ni mogoče dokazati z navajanjem, da je bilo merilo „upravičenega interesa“, ki ga je v skladu z Direktivo o preprečevanju pranja denarja v različici, ki je veljala pred spremembo z Direktivo 2018/843, moral imeti vsakdo, ki je želel dostopati do informacij o dejanskih lastnikih, težko izvajati in da bi njegova uporaba lahko privedla do arbitrarnih odločitev. Morebiten obstoj težav pri natančni opredelitvi primerov in pogojev, v katerih ima javnost lahko dostop do informacij o dejanskih lastnikih, namreč ne more upravičiti tega, da zakonodajalec Unije določi dostop širše javnosti do teh informacij.

Na drugi strani, s pojasnili iz Direktive 2018/843 se prav tako ne more dokazati nujna potrebnost zadevnega poseganja.[26] V zvezi s tem, da naj bi v skladu s temi pojasnili dostop širše javnosti do informacij o dejanskih lastnikih civilni družbi, zlasti tisku in organizacijam civilne družbe, omogočal boljši nadzor informacij, je Sodišče navedlo, da imajo tako tisk kot organizacije civilne družbe, ki so povezane s preprečevanjem pranja denarja in financiranja terorizma ter bojem proti njima, upravičen interes za dostop do zadevnih informacij. Enako velja za osebe, ki želijo poznati identiteto dejanskih lastnikov gospodarskega ali drugega pravnega subjekta, ker bi z njimi lahko sklepale transakcije, ali tudi za finančne institucije in organe, ki sodelujejo v boju proti kaznivim dejanjem na področju pranja denarja ali financiranja terorizma.

Poleg tega zadevno poseganje tudi ni sorazmerno. V zvezi s tem Sodišče ugotavlja, da materialnopravna pravila, ki zamejujejo to poseganje, ne ustrezajo zahtevi po jasnosti in natančnosti. Spremenjena Direktiva o preprečevanju pranja denarja namreč določa, da se vsem članom širše javnosti dovoli dostop „vsaj“ do podatkov iz te direktive, in državam članicam daje možnost, da omogočijo dostop do dodatnih informacij, ki vključujejo „vsaj“ datum rojstva ali kontaktne podatke zadevnega dejanskega lastnika. Z uporabo izraza „vsaj“ pa ta direktiva dovoljuje, da se javnosti omogoči dostop do podatkov, ki niso dovolj opredeljeni niti določljivi.

Poleg tega Sodišče, kar zadeva uravnoteženost teže tega poseganja s pomenom zastavljenega cilja splošnega interesa, priznava, da je glede na pomen tega cilja z njim mogoče utemeljiti poseganja, tudi resna, v temeljne pravice, določene v členih 7 in 8 Listine.

[26] To se nanaša na pojasnila iz uvodne izjave 30 Direktive 2018/843.

Vendar so, na eni strani, za boj proti pranju denarja in financiranju terorizma odgovorni predvsem javni organi in subjekti, kot so kreditne ali finančne ustanove, ki so jim zaradi njihovih dejavnosti naložene specifične obveznosti na tem področju. Zato spremenjena Direktiva o preprečevanju pranja denarja določa, da morajo biti informacije o dejanskih lastnikih vedno dostopne pristojnim organom in finančnim obveščevalnim enotam, brez kakršne koli omejitve, ter pooblaščenim subjektom, in sicer v okviru skrbnega preverjanja strank.[27]

Na drugi strani, v primerjavi s prejšnjo ureditvijo, ki je poleg dostopa pristojnih organov in nekaterih subjektov do informacij o dejanskih lastnikih določala dostop vseh oseb ali organizacij, ki lahko izkažejo upravičen interes, ureditev, uvedena z Direktivo 2018/843, pomeni bistveno hujšo kršitev temeljnih pravic, zagotovljenih s členoma 7 in 8 Listine, ne da bi bila ta zaostritev lahko izravnana z morebitnimi koristmi, ki bi lahko izhajale iz te druge ureditve v primerjavi s prvo, kar zadeva boj proti pranju denarja in financiranju terorizma.

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)

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.

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.

[27] Člen 30(5), prvi pododstavek, točki (a) in (b), spremenjene Direktive o preprečevanju pranja denarja.

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 ureditev presega meje nujno potrebnega in je ni mogoče šteti za upravičeno v demokratični družbi, kot to zahteva navedeni člen 15(1) ob upoštevanju zgoraj navedenih členov Listine.

Navedena določba v povezavi z istimi členi 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.

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.

II. Obdelava osebnih podatkov v smislu splošne ureditve s tega področja

1. Področje uporabe splošne ureditve

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[28], 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[29] 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 navedena 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.

Glede odločbe 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 upoštevala v odločbi o ustreznosti, povsem drugo naravo. Ta odločba se namreč ni nanašala na obdelavo podatkov, potrebno za

[28] 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).

[29] 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 iz PNR s strani letalskih prevoznikov Uradu za carine in zaščito meja pri Ministrstvu Združenih držav za domovinsko varnost (UL 2004, L 183, str. 83 in popravek v UL 2005, L 255, str. 168).

opravljanje storitev, ampak na obdelavo podatkov, ki se šteje za nujno za zaščito javne varnosti in za namene kazenskega pregona.

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.

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.

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.

Sodišče je v tej sodbi 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.

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.

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

F. Ryneš je zaradi vrste napadov namestil nadzorno kamero na svojo hišo. 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 podatkov, ki ni zajeta v Direktivi 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 shranjuje na napravo za neprekinjeno snemanje, 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.

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. Poleg tega je že v besedilu te določbe uporaba Direktive 95/46 izključena za obdelavo podatkov, opravljeno 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.

Sodba z dne 16. januarja 2024 (veliki senat), Österreichische Datenschutzbehörde (C-33/22, EU:C:2024:46)

Nationalrat (državni svet, Avstrija) je za preučitev morebitnega političnega vpliva na Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (zvezni urad za varstvo ustave in boj proti terorizmu, Avstrija)[30] ustanovil preiskovalno komisijo (v nadaljevanju: preiskovalna komisija v zvezi z BVT). Ta komisija je zaslišala WK kot pričo. Kljub njegovi zahtevi za anonimizacijo je bil zapisnik njegovega zaslišanja, v katerem so bili navedeni njegovi popolni priimek in imena, objavljen na spletnem mestu Parlament Österreich (avstrijski parlament). WK je pri Österreichische Datenschutzbehörde (organ za varstvo podatkov, Avstrija, v nadaljevanju: Datenschutzbehörde) vložil pritožbo, v kateri je trdil, da je tako razkritje njegove identitete v nasprotju s SUVP in avstrijsko zakonodajo. Datenschutzbehörde se je z odločbo z dne 18. septembra 2019 izrekel za nepristojnega za odločanje o pritožbi, in sicer je pojasnil, da načelo delitve oblasti izključuje, da bi kot organ izvršilne oblasti lahko nadziral preiskovalno komisijo v zvezi BVT, ki je del zakonodajne oblasti.

Po odločbi Bundesverwaltungsgericht (zvezno upravno sodišče, Avstrija), ki je ugodilo pravnemu sredstvu WK in odpravilo odločbo Datenschutzbehörde, je ta organ pri vrhovnem upravnem sodišču vložil revizijo zoper odločbo zveznega upravnega sodišča.

V tem okviru je predložitveno sodišče Sodišču postavilo vprašanje, ali dejavnosti preiskovalne komisije, ki jo ustanovi parlament države članice, spadajo na področje uporabe SUVP in ali se ta uredba uporablja, kadar se te dejavnosti nanašajo na zaščito nacionalne varnosti.

Na prvem mestu, Sodišče je opozorilo, da je edini namen člena 2(2)(a) SUVP, ki določa, da se ta uredba ne uporablja za obdelavo osebnih podatkov v okviru dejavnosti zunaj področja uporabe prava Unije, izključiti s področja uporabe te uredbe obdelave osebnih podatkov, ki jih izvajajo državni organi v okviru dejavnosti, katere namen je ohranjanje nacionalne varnosti, ali v okviru dejavnosti, ki jo je mogoče razvrstiti v isto kategorijo. Tako zgolj dejstvo, da je dejavnost značilna za državo ali državni organ, ne zadostuje za samodejno izključitev uporabe SUVP za to dejavnost.

To razlago, ki izhaja iz neobstoja razlikovanja glede na identiteto avtorja zadevne obdelave, potrjuje člen 4, točka 7, SUVP[31].

Sodišče je pojasnilo, da parlamentarna narava preiskovalne komisije v zvezi z BVT ne pomeni, da so njene dejavnosti izključene s področja uporabe SUVP. Izjema iz člena 2(2)(a) te uredbe se namreč nanaša le na kategorije dejavnosti, ki zaradi svoje narave ne spadajo na področje uporabe prava Unije, ne pa na kategorije oseb. Zato okoliščina, da obdelavo osebnih podatkov izvaja preiskovalna komisija, ki jo je ustanovil

[30] Ta subjekt je 1. decembra 2021 postal Direktion Staatsschutz und Nachrichtendienst (direktorat za državno varnost in obveščevalne službe, Avstrija).

[31] Ta opredeljuje, da pojem „upravljavec“ pomeni „fizično ali pravno osebo, javni organ, agencijo ali drugo telo, ki samo ali skupaj z drugimi določa namene in sredstva obdelave“.

parlament države članice zaradi izvajanja svoje pristojnosti nadzora nad izvršilno oblastjo, sama po sebi ne omogoča ugotovitve, da se ta obdelava izvaja v okviru dejavnosti zunaj področja uporabe prava Unije.

Na drugem mestu, Sodišče je navedlo, da čeprav so države članice pristojne, da opredelijo svoje bistvene varnostne interese in sprejmejo ustrezne ukrepe za zagotovitev varnosti,[32] zgolj dejstvo, da je bil nacionalni ukrep sprejet zaradi zaščite nacionalne varnosti, ne more povzročiti neuporabe prava Unije in držav članic oprostiti obveznosti spoštovanja tega prava. Izjema iz člena 2(2)(a) SUVP pa se nanaša le na kategorije dejavnosti, ki zaradi svoje narave ne spadajo na področje uporabe prava Unije. V zvezi s tem okoliščina, da je upravljavec javni organ, katerega glavna dejavnost je zagotavljanje nacionalne varnosti, sama po sebi ne more zadostovati za to, da se s področja uporabe SUVP izključijo obdelave osebnih podatkov, ki jih ta organ izvaja v okviru svojih drugih dejavnosti.

V obravnavani zadevi se zdi, da politični nadzor, ki ga izvaja preiskovalna komisija v zvezi z BVT, sam po sebi ne pomeni dejavnosti, katere namen je ohraniti nacionalno varnost ali ki spada v isto kategorijo. Zato ta dejavnost ni izključena s področja uporabe SUVP, kar pa mora preveriti predložitveno sodišče.

Kljub temu ima lahko parlamentarna preiskovalna komisija dostop do osebnih podatkov, ki morajo biti iz razlogov nacionalne varnosti deležni posebnega varstva. V zvezi s tem se lahko z zakonodajnimi ukrepi določijo omejitve pravic in obveznosti iz SUVP za zagotovitev med drugim nacionalne varnosti.[33] Tako je mogoče na tej podlagi utemeljiti omejitve glede zbiranja osebnih podatkov, obveščanja posameznikov, na katere se nanašajo osebni podatki, in njihovega dostopa do navedenih podatkov ali razkritja teh podatkov brez privolitve posameznikov, na katere se nanašajo osebni podatki, drugim osebam kot upravljavcu, če take omejitve spoštujejo bistvo temeljnih pravic in svoboščin posameznikov, na katere se nanašajo osebni podatki, ter pomenijo potreben in sorazmeren ukrep v demokratični družbi.

Vendar je Sodišče opozorilo, da iz informacij, ki so mu bile dane na voljo, ni razvidno, da bi preiskovalna komisija v zvezi z BVT trdila, da je bilo razkritje osebnih podatkov posameznika, na katerega se nanašajo osebni podatki, potrebno za zaščito nacionalne varnosti in je temeljilo na za to določenem nacionalnem zakonodajnem ukrepu, kar pa mora po potrebi preveriti predložitveno sodišče.

[32] V skladu s členom 4(2) PEU.
[33] Člen 23 SUVP.

2. Pojem „osebni podatki“

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

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.

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.

Sodba z dne 20. decembra 2017, Nowak (C-434/16, 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 ima subjekt, ki organizira izpit, v tem primeru zbornica računovodij, finančnikov in revizorjev, potrebne informacije, na podlagi katerih 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, na primer, možnosti dostopa do želenega poklica oziroma zaposlitve. Ugotovitev, da so pisni odgovori, ki jih je na poklicnem izpitu dal kandidat, informacije, ki se nanj nanašajo zaradi svoje vsebine, namena in posledic, velja, tudi kadar gre za izpit z dostopnimi viri.

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

Četrtič, Sodišče je razsodilo, da so lahko pisni odgovori, ki jih je na poklicnem izpitu dal kandidat, in morebitni komentarji popravljavca, ki so s temi odgovori povezani, predmet preverjanja, zlasti glede njihove točnosti in nujnosti njihovega shranjevanja v smislu

člena 6(1)(d) in (e) Direktive 95/46, 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.

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.

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 je te podatke 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. Taka obdelava osebnih podatkov za opravljanje prostovoljnih ali verskih dejavnosti namreč ne spada k nobeni od izjem od področja uporabe navedene 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 navedene direktive.

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

V tej sodbi (glej tudi razdelek II.1., naslovljen „Področje uporabe splošne ureditve“) je Sodišče pojasnilo 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. Sodišče je poleg tega spomnilo, da je treba postopke iz navedene direktive šteti za obdelavo, tudi če se nanašajo izključno na informacije, ki so že objavljene v medijih. Splošna izjema od uporabe te direktive v tem primeru bi povzročila, da bi ta direktiva v veliki meri izgubila smisel.

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

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.

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[34] 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 SUVP. Tako je Sodišču predlagalo, naj pojasni obseg več določb SUVP, 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]“[35], za katero SUVP določa povečano varstvo zaradi posebne občutljivosti zadevnih podatkov.

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 SUVP. To področje uporabe je namreč zelo široko in ta obdelava ne spada med izjeme od uporabe te uredbe.

Tako na eni strani za to obdelavo ne velja izjema, na podlagi katere se SUVP ne uporablja za obdelavo, opravljeno v okviru dejavnosti, ki ne spada na področje uporabe prava Unije.[36] 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.

Na drugi strani posredovanje osebnih podatkov v zvezi s kazenskimi točkami prav tako ni obdelava, zajeta z izjemo, na podlagi katere se SUVP ne uporablja za obdelavo osebnih podatkov, ki jo opravljajo organi, pristojni v kazenskih zadevah.[37] Sodišče je namreč ugotovilo, da CSDD pri izvajanju navedenega posredovanja ni mogoče šteti za tak „pristojni organ“.[38]

---

34 Člen 14[1](2) Ceļu satiksmes likums (zakon o cestnem prometu) z dne 1. oktobra 1997 (Latvijas Vēstnesis, 1997, št. 274/276).

35 Člen 10 SUVP.

36 Člen 2(2)(a) SUVP.

37 Člen 2(2)(d) SUVP.

38 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).

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]“,[39] ki uživajo povečano varstvo, je ob opiranju med drugim na zgodovino nastanka SUVP 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 SUVP. 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.

Sodba z dne 5. decembra 2023 (veliki senat), Nacionalinis visuomenės sveikatos centras (C-683/21,* EU:C:2023:949*)

Leta 2020 so se litovski organi za boljše obvladovanje pandemije covida-19 odločili organizirati nakup mobilne aplikacije informacijske tehnologije. Ta aplikacija naj bi prispevala k epidemiološkemu spremljanju, tako da bi omogočila beleženje in spremljanje podatkov oseb, izpostavljenih virusu, ki povzroča covid-19.

Zato je Nacionalinis visuomenės sveikatos centras prie Sveikatos apsaugos ministerijos (nacionalni center za javno zdravje pri ministrstvu za zdravje, Litva, v nadaljevanju: CNSP), pooblaščen za ta nakup, stopil v stik z družbo UAB „IT sprendimai sėkmei“ (v nadaljevanju: družba ITSS) in jo pozval, naj tako mobilno aplikacijo razvije. Nato so zaposleni v CNSP tej družbi poslali elektronska sporočila, ki so se nanašala med drugim na vprašanja, ki bi morala biti vključena v to aplikacijo.

V obdobju od aprila do maja 2020 je bila mobilna aplikacija, ki jo je razvila družba ITSS, dostopna javnosti. Tako je to aplikacijo uporabilo 3802 oseb, ki so posredovale različne podatke, ki so se nanašali nanje in ki so bili zahtevani pri uporabi te aplikacije. Vendar

[39] Člen 10 SUVP.

CNSP zaradi pomanjkanja sredstev družbi ITSS ni oddal nobenega javnega naročila za uradni nakup njene mobilne aplikacije in je postopek v zvezi s tem ustavil.

Medtem je nacionalni nadzorni organ začel preiskavo v zvezi z obdelavo osebnih podatkov, ki izhaja iz uporabe te aplikacije. Z odločbo tega organa, sprejeto na podlagi preiskave, je bila upravna globa naložena tako CNSP kot družbi ITSS, ki se je štela za skupnega upravljavca.

CNSP je to odločbo izpodbijal pri Vilniaus apygardos administracinis teismas (regionalno upravno sodišče v Vilni, Litva). Ker je to sodišče dvomilo o razlagi več določb SUVP, je pri Sodišču vložilo predlog za sprejetje predhodne odločbe.

Sodišče, ki je zasedalo v velikem senatu, je v sodbi med drugim pojasnilo pojem „obdelava“. V zvezi s tem je navedlo, da uporaba osebnih podatkov za računalniško testiranje mobilne aplikacije pomeni obdelavo v smislu SUVP. Drugače pa je, če so taki podatki anonimizirani tako, da posameznik, na katerega se ti podatki nanašajo, ni ali ni več določljiv, ali če gre za fiktivne podatke, ki se ne nanašajo na obstoječo fizično osebo.

Na eni strani namreč vprašanje, ali se osebni podatki uporabljajo za računalniško testiranje ali za drug namen, ne vpliva na opredelitev dejanja kot „obdelave“. Na drugi strani je mogoče le obdelavo, ki se nanaša na osebne podatke, opredeliti kot „obdelavo“ v smislu SUVP. Fiktivni ali anonimni podatki pa niso osebni podatki.

4. Pojem „zbirka osebnih podatkov“

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

5. Pojem „upravljavec osebnih podatkov“

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

Sodišče se je v tej zadevi (glej tudi razdelka II.3. in II.4., naslovljena „Pojem ‚obdelava osebnih podatkov‘“ in „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.

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

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.

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 mesto.

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).

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.

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.

Sodba z dne 5. decembra 2023 (veliki senat), Nacionalinis visuomenės sveikatos centras (C-683/21, EU:C:2023:949***)***

Sodišče je v tej zadevi (glej tudi razdelek II.3., naslovljen „Pojem ‚obdelava osebnih podatkov‘“) navedlo, da je subjekt, ki je podjetju naložil razvoj mobilne aplikacije informacijske tehnologije ter je v tem okviru sodeloval pri določitvi namenov in sredstev

obdelave osebnih podatkov, ki se izvede s to aplikacijo, mogoče šteti za upravljavca.[40] Te ugotovitve ni mogoče ovreči z dejstvom, da ta subjekt sam ni izvedel dejanj obdelave takih podatkov, ni izrecno dal soglasja za izvedbo konkretnih dejanj take obdelave ali za dajanje navedene mobilne aplikacije na voljo javnosti ter ni kupil te mobilne aplikacije, razen če je navedeni subjekt pred tem dajanjem na voljo javnosti izrecno nasprotoval takemu dajanju na voljo in obdelavi osebnih podatkov, ki je iz tega izhajala.

6. Pojem „skupni upravljavec“

Sodba z dne 5. decembra 2023 (veliki senat), Nacionalinis visuomenės sveikatos centras (C-683/21, EU:C:2023:949)

Sodišče je v tej zadevi (glej tudi razdelka II.3. in II.5., naslovljena „Pojem ‚obdelava osebnih podatkov‘“ in „Pojem ‚upravljavec osebnih podatkov‘“) ugotovilo, da se pri opredelitvi dveh subjektov kot skupnih upravljavcev ne zahteva obstoj dogovora med tema subjektoma o določitvi namenov in sredstev obdelave osebnih podatkov niti obstoj dogovora, ki določa pogoje v zvezi s skupnim upravljanjem. V skladu s SUVP[41] morajo sicer skupni upravljavci z medsebojnim dogovorom na pregleden način določiti svoje dolžnosti za zagotovitev skladnosti z zahtevami iz te uredbe. Vendar obstoj takega dogovora ni poglavitni pogoj za opredelitev dveh ali več subjektov kot „skupnih upravljavcev“, temveč obveznost, ki je s SUVP naložena skupnim upravljavcem, ko so enkrat opredeljeni kot taki, da se zagotovi spoštovanje zahtev iz te uredbe, ki veljajo zanje. Tako ta opredelitev izhaja zgolj iz dejstva, da je več subjektov sodelovalo pri določitvi namenov in sredstev obdelave.

Glede skupne določitve namenov in sredstev obdelave s strani zadevnih subjektov je Sodišče pojasnilo, da ima lahko njihovo sodelovanje pri tej določitvi več različnih oblik in se lahko odraža v skupni odločitvi ali pa temelji na njihovih podobnih odločitvah. Vendar se morajo v zadnjenavedenem primeru te odločitve med seboj dopolnjevati, tako da ima vsaka od njih dejanski učinek na določitev namenov in sredstev obdelave.

7. Pogoji zakonitosti obdelave osebnih podatkov

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

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

[40] V smislu člena 4, točka 7, SUVP.

[41] Člen 26(1) SUVP v povezavi z uvodno izjavo 79 te uredbe.

tujcev, ki na nemškem ozemlju prebivajo več kot tri mesece. Register se je uporabljal za statistične namene in pri izvajanju pristojnosti varnostnih služb, policije in sodnih organov na področju pregona in preiskav v zvezi s kaznivimi ravnanji ali ogrožanjem javne varnosti.

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

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

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

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, nujna za statistične namene.

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.

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.

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 riaditel'stvo (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.

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.

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.

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.

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[42] 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.[43] Glede tega velja, da privolitev ni veljavna v primeru molka, vnaprej označenih okenc ali nedejavnosti.

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, ga pogodbene določbe ne smejo zavesti glede možnosti sklenitve pogodbe, tudi če zavrne privolitev v obdelavo svojih podatkov.

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.

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

[42] Člen 7 Direktive 95/46 in člen 6 SUVP.
[43] Člen 2(h) Direktive 95/46 in člen 4, točka 11, SUVP.

obdelavo svojih osebnih podatkov, ne more zahtevati od teh strank, da aktivno izjavijo svojo zavrnitev.

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 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.

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

Sodišče je v tej sodbi (glej tudi razdelek II.3., naslovljen „Pojem ‚obdelava osebnih podatkov‘“) razsodilo, da SUVP 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.

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“.[44] 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

[44] V skladu s členom 6(1)(e) SUVP je obdelava osebnih podatkov zakonita, če je „potrebna za opravljanje naloge v javnem interesu […]“.

lahko povzroči neodobravanje družbe in stigmatizacijo posameznika, na katerega se osebni podatki nanašajo.

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.

Sodišče je prav tako iz enakih razlogov razsodilo, da SUVP 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.

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.

III. Obdelava osebnih podatkov v smislu sektorskih predpisov

1. Obdelava osebnih podatkov na področju elektronskih komunikacij

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

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.

Sodišče je v tem okviru pojasnilo, da je sicer v sodbi Tele2 Sverige ter Watson in drugi[45] 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.

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 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“.

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)

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,

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

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.

Dalje, Sodišče je opozorilo, da Direktiva 2002/58[46] 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,[47] le ob upoštevanju splošnih načel prava Unije, med katerimi je načelo sorazmernosti, in temeljnih pravic, zagotovljenih z Listino[48].

V tem okviru je Sodišče po eni strani v zadevi Privacy International ugotovilo, da Direktiva 2002/58 v povezavi z Listino nasprotuje nacionalni ureditvi, s katero je ponudnikom elektronskih komunikacijskih storitev zaradi zaščite nacionalne varnosti naloženo 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) SUVP v povezavi z Listino tako,

[46] Člen 15(1) in (3) Direktive 2002/58.
[47] Člen 5(1) Direktive 2002/58.
[48] Zlasti členi 7, 8 in 11 ter člen 52(1) Listine.

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.

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.

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.

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.

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 v povezavi z Listino.

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.

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 osebo 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[49].

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“ upravni organ v smislu sodbe Tele2 Sverige ter Watson in drugi,[50] 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,

[49] Natančneje, s členom 15(1) Direktive 2002/58 v povezavi s členi 7, 8 in 11 ter členom 52(1) Listine.

[50] 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).

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.

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.

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.

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.

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.

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.

Sodba z dne 5. aprila 2022, Commissioner of An Garda Síochána in drugi (C-140/20, EU:C:2022:258)

V tej zadevi je predlog za sprejetje predhodne odločbe vložilo Supreme Court (vrhovno sodišče, Irska) v okviru civilnega postopka, ki ga je vložila oseba, obsojena na dosmrtni zapor zaradi umora, storjenega na Irskem. Zadnjenavedena je izpodbijala skladnost nekaterih določb nacionalne zakonodaje, ki se nanašajo na hrambo splošnih podatkov v okviru elektronskih komunikacij, s pravom Unije. Na podlagi tega zakona so ponudniki storitev elektronskih komunikacij hranili podatke o prometu in podatke o lokaciji v zvezi s telefonskimi klici obdolženca ter policijskim organom omogočili dostop do njih. Predložitveno sodišče je dvomilo zlasti glede skladnosti splošne in neselektivne ureditve hrambe teh podatkov v zvezi z bojem proti hudim kaznivim dejanjem z Direktivo 2002/58 v povezavi z Listino.

Sodišče je v sodbi, ki jo je izrekel veliki senat, potrdilo sodno prakso, ki izhaja iz sodbe La Quadrature du Net in drugi[51], in natančno opredelilo njen obseg ter opozorilo, da splošna in neselektivna hramba podatkov o prometu in podatkov o lokaciji, povezanih z elektronskimi komunikacijami, ni dovoljena zaradi boja proti hudemu kriminalu in

[51] Sodba z dne 6 oktobra 2020, La Quadrature du Net in drugi (C-511/18, C-512/18 in C-520/18, EU:C:2020:791).

preprečevanja resnih groženj za javno varnost. Potrdilo je tudi sodno prakso, ki izhaja iz sodbe Prokuratuur (Pogoji za dostop do podatkov o elektronskih komunikacijah)[52], zlasti glede obveznosti, da se dostop pristojnih nacionalnih organov do navedenih hranjenih podatkov pogojuje s predhodnim nadzorom glede policijskega uradnika, ki ga opravi bodisi sodišče bodisi neodvisen upravni organ.

Prvič, Sodišče je presodilo, da Direktiva 2002/58 v povezavi z Listino nasprotuje zakonskim ukrepom, ki preventivno, in sicer zaradi boja proti hudemu kriminalu in preprečevanja resnih groženj javni varnosti, določajo splošno in neselektivno hrambo podatkov o prometu in podatkov o lokaciji. Namreč, ob upoštevanju na eni strani odvračilnih učinkov na uresničevanje temeljnih pravic[53], ki jih ta hramba lahko povzroči, in na drugi strani resnosti posega, ki ga ta hramba pomeni, mora biti taka hramba v ureditvi, ki jo vzpostavlja ta direktiva, izjema, in ne pravilo, zato ti podatki ne morejo biti predmet sistematične in nepretrgane hrambe. Kriminala, tudi posebej hudega, ni mogoče enačiti z grožnjo za nacionalno varnost, ker bi taka izenačitev lahko pomenila vmesno kategorijo med nacionalno varnostjo in javno varnostjo, da bi se za drugo uporabile zahteve, ki so neločljivo povezane s prvo.

Nasprotno pa Direktiva 2002/58 v povezavi z Listino ne nasprotuje zakonskim ukrepom, ki za boj proti hudemu kriminalu in preprečevanje resnih groženj javni varnosti določajo ciljno hrambo podatkov o prometu in podatkov o lokaciji, ki je na podlagi objektivnih in nediskriminatornih elementov časovno omejena glede na kategorije oseb, na katere se nanašajo osebni podatki, ali glede na geografsko merilo, za obdobje, ki je nujno potrebno, vendar ga je mogoče podaljšati. Dodalo je, da lahko tak ohranitveni ukrep, ki se nanaša na kraje ali infrastrukture, ki jih redno obiskuje zelo veliko ljudi, ali strateške kraje, kot so letališča, železniške postaje, pomorska pristanišča ali cestninska območja, pristojnim organom omogoči, da pridobijo informacije o prisotnosti oseb na teh krajih ali geografskih območjih, ki tam uporabljajo elektronsko komunikacijsko sredstvo, in da na podlagi tega ugotavljajo njihovo navzočnost in dejavnosti na navedenih krajih ali geografskih območjih zaradi boja proti hudemu kriminalu. Vsekakor morebitni obstoj težav pri natančni opredelitvi primerov in pogojev, pod katerimi se lahko opravi ciljna hramba, nikakor ne more upravičiti tega, da države članice z uvedbo izjeme določijo splošno in neselektivno hrambo podatkov o prometu in podatkov o lokaciji.

Ta direktiva v povezavi z Listino prav tako ne nasprotuje zakonskim ukrepom, ki za isti namen določajo splošno in neselektivno hrambo naslovov IP, dodeljenih viru povezave, za obdobje, ki je časovno omejeno na to, kar je nujno potrebno, in podatkov o civilni identiteti uporabnikov elektronskih komunikacij. V zvezi s tem zadnjim vidikom je Sodišče natančneje pojasnilo, da niti Direktiva 2002/58 niti noben drug akt prava Unije ne nasprotujeta nacionalni zakonodaji, katere cilj je boj proti hudemu kriminalu in v skladu s katero je pridobitev elektronskega komunikacijskega sredstva, kot je predplačljiva kartica SIM, pogojena s preverjanjem uradnih dokumentov, iz katerih je

[52] Sodba z dne 2. marca 2021, Prokuratuur (Pogoji za dostop do podatkov o elektronskih komunikacijah, C-746/18, *EU:C:2021:152*).
[53] Določenih v členih od 7 do 11 Listine.

razvidna identiteta kupca, in z registracijo informacij, ki iz tega izhajajo, zato mora prodajalec, če je to potrebno, pristojnim nacionalnim organom omogočiti dostop do teh informacij.

Enako velja za zakonske ukrepe, ki za boj proti hudemu kriminalu in za zaščito nacionalne varnosti določajo uporabo odredbe, s katero je ponudnikom elektronskih komunikacijskih storitev prek sklepa pristojnega organa, ki je predmet učinkovitega sodnega nadzora, za določeno obdobje naložena takojšnja hramba („quick freeze“) podatkov o prometu in podatkov o lokaciji, s katerimi ti ponudniki razpolagajo. Le boj proti hudemu kriminalu in *a fortiori* zaščita nacionalne varnosti lahko namreč upravičita tako hrambo, če ta ukrep in dostop do hranjenih podatkov spoštujeta meje nujno potrebnega. Sodišče je opozorilo, da se tak ukrep hitre hrambe lahko razširi na podatke o prometu in podatke o lokaciji, ki se nanašajo na osebe, za katere se ne domneva, da so načrtovale ali storile hudo kaznivo dejanje ali ogrožale nacionalno varnost, če lahko ti podatki na podlagi objektivnih in nediskriminatornih elementov prispevajo k razjasnitvi takega kaznivega dejanja ali ogrožanja nacionalne varnosti, kot na primer podatki žrtve tega dejanja in podatki o njenih gospodarskih ali socialnih okoliščinah.

Vendar je Sodišče v nadaljevanju navedlo, da morajo vsi zgoraj navedeni zakonski ukrepi z jasnimi in natančnimi pravili zagotoviti, da je hramba zadevnih podatkov pogojena s spoštovanjem zadevnih materialnih in postopkovnih pogojev ter da imajo zadevne osebe na voljo učinkovita jamstva proti tveganjem zlorabe. Različni ukrepi hrambe podatkov o prometu in podatkov o lokaciji se lahko v skladu z odločitvijo nacionalnega zakonodajalca in ob spoštovanju meja tega, kar je nujno potrebno, uporabijo skupaj.

Poleg tega je Sodišče pojasnilo, da je za boj proti hudemu kriminalu dostop do teh podatkov, ki se hranijo splošno in neselektivno, da bi se zoperstavili resni grožnji za nacionalno varnost, v nasprotju s hierarhijo ciljev v splošnem interesu, ki lahko upravičijo ukrep, sprejet na podlagi Direktive 2002/58. S tem bi se namreč dopustilo, da se lahko dostop upraviči s ciljem, ki je manj pomemben kot cilj, ki je upravičil hrambo, in sicer zaščita nacionalne varnosti, s čimer pa se lahko prepovedi splošne in neselektivne hrambe zaradi boja proti hudemu kriminalu odvzame polni učinek.

Drugič, Sodišče je presodilo, da Direktiva 2002/58 v povezavi z Listino nasprotuje nacionalni ureditvi, v skladu s katero se centralizirana obdelava prošenj za dostop do podatkov, ki jih hranijo ponudniki elektronskih komunikacijskih storitev, ki jih poda policija v okviru preiskovanja in pregona hudih kaznivih dejanj, naloži policijskemu uradniku – tudi če mu pomaga enota policije, ki ima določeno stopnjo samostojnosti pri opravljanju svojih nalog – nad odločitvami katerega se lahko pozneje opravi sodni nadzor. Na eni strani namreč tak uradnik ne izpolnjuje zahtev po neodvisnosti in nepristranskosti, ki veljajo za upravni organ, ki izvaja predhodni nadzor nad zahtevami pristojnih nacionalnih organov za dostop do podatkov, saj v razmerju do teh organov nima statusa tretje osebe. Na drugi strani, čeprav je odločba takega uradnika lahko predmet naknadnega sodnega nadzora, ta nadzor ne more nadomestiti neodvisnega nadzora in, razen v ustrezno utemeljenih nujnih primerih, predhodnega nadzora.

Tretjič, Sodišče je nazadnje potrdilo svojo sodno prakso, v skladu s katero pravo Unije nasprotuje temu, da nacionalno sodišče časovno omeji učinke ugotovitve neveljavnosti, ki jo mora v skladu z nacionalnim pravom podati glede nacionalne zakonodaje, ki ponudnikom elektronskih komunikacijskih storitev nalaga splošno in neselektivno hrambo podatkov o prometu in podatkov o lokaciji, ker ta zakonodaja ni združljiva z Direktivo 2002/58. Ob tem je Sodišče opozorilo, da dopustnost dokazov, pridobljenih s tako hrambo, v skladu z načelom procesne avtonomije držav članic spada v nacionalno pravo, če se upoštevata zlasti načeli enakovrednosti in učinkovitosti.

Sodba z dne 20. septembra 2022 (veliki senat), VD in SR (C-339/20 in C-397/20, EU:C:2022:703)

Zoper VD in SR, fizični osebi, obtoženi kaznivih dejanj trgovanja na podlagi notranjih informacij, prikrivanja kaznivih dejanj trgovanja na podlagi notranjih informacij, sostorilstva, korupcije in pranja denarja, sta bila po preiskavi Autorité des marchés financiers (organ za finančne trge, AMF, Francija, v nadaljevanju: AMF) začeta kazenska postopka. V okviru te preiskave je AMF uporabil osebne podatke, ki izhajajo iz telefonskih klicev VD in SR ter ki so v okviru opravljanja elektronskih komunikacijskih storitev nastali na podlagi zakonika o pošti in elektronskih komunikacijah.

Ker je njuna obtožnica temeljila na podatkih o prometu, ki jih je predložil AMF, sta VD in SR pri cour d'appel de Paris (višje sodišče v Parizu, Francija) vsak posebej vložila pritožbi in med drugim navedla pritožbeni razlog, ki se v bistvu nanaša na kršitev člena 15(1) Direktive 2002/58 v povezavi s členi 7, 8 in 11 ter členom 52(1) Listine. Natančneje, VD in SR sta s sklicevanjem na sodno prakso, ki izhaja iz sodbe Tele2 Sverige ter Watson in drugi[54], izpodbijala to, da se je AMF pri zbiranju navedenih podatkov oprl na zadevne nacionalne določbe, čeprav po njunem mnenju, prvič, te določbe niso bile v skladu s pravom Unije, ker so določale splošno in neselektivno hrambo podatkov o prometu, in drugič, niso predpisovale nobene omejitve glede pooblastila za preiskovalce AMF, da se jim posredujejo hranjeni podatki.

Cour d'appel de Paris (višje sodišče v Parizu) je s sodbama z dne 20. decembra 2018 in 7. marca 2019 pritožbi VD in SR zavrnilo. Za zavrnitev zgoraj navedenega pritožbenega razloga se je drugostopenjsko sodišče oprlo zlasti na to, da Uredba o zlorabi trga[55] pristojnim organom omogoča, da – kolikor to dovoljuje nacionalno pravo – zahtevajo posredovanje obstoječih zapisov podatkov o prometu, ki jih imajo operaterji storitev elektronskih komunikacij, če obstaja razlog za sum kršitve prepovedi trgovanja na podlagi notranjih informacij in če so taki zapisi lahko upoštevni za preiskavo v zvezi s to kršitvijo.

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

[55] Uredba (EU) št. 596/2014 Evropskega parlamenta in Sveta z dne 16. aprila 2014 o zlorabi trga (uredba o zlorabi trga) ter razveljavitvi Direktive 2003/6/ES Evropskega parlamenta in Sveta ter direktiv Komisije 2003/124/ES, 2003/125/ES in 2004/72/ES (UL 2014, L 173, str. 1).

VD in SR sta nato pri Cour de cassation (kasacijsko sodišče, Francija), ki je predložitveno sodišče v obravnavanih zadevah, vložila pritožbo.

V teh okoliščinah je to sodišče spraševalo o uskladitvi člena 15(1) Direktive 2002/58 v povezavi z Listino z zahtevami, ki izhajajo iz člena 12(2)(a) in (d) Direktive o zlorabi trga[56] ter člena 23(2)(g) in (h) Uredbe o zlorabi trga. To spraševanje izhaja iz zakonodajnih ukrepov iz postopka v glavni stvari, ki zaradi boja proti kaznivim dejanjem zlorabe trga, katerih del je trgovanje na podlagi notranjih informacij, za operaterje elektronskih komunikacijskih storitev preventivno določajo splošno in neselektivno hrambo podatkov o prometu za eno leto od dneva njihovega zapisa. Predložitveno sodišče je za primer, da bi Sodišče odločilo, da zakonodaja o hrambi zadevnih podatkov o povezavi iz postopka v glavni stvari ni v skladu s pravom Unije, spraševalo o začasni ohranitvi učinkov te zakonodaje, da bi se preprečila pravna negotovost in omogočilo, da se predhodno zbrani in shranjeni podatki uporabijo za odkrivanje in pregon trgovanja na podlagi notranjih informacij.

Sodišče, ki je zasedalo v velikem senatu, je v sodbi razsodilo, da splošna in neselektivna hramba podatkov o prometu za eno leto od dneva, ko so jih operaterji elektronskih komunikacijskih storitev registrirali, in sicer preventivno zaradi boja proti kaznivim dejanjem zlorabe trga, ni dovoljena. Poleg tega je potrdilo svojo sodno prakso, v skladu s katero pravo Unije nasprotuje temu, da nacionalno sodišče časovno omeji učinke ugotovitve neveljavnosti, ki jo mora podati glede nacionalnih zakonodajnih določb, ki niso združljive s pravom Unije.

Sodišče je najprej opozorilo, da je treba za razlago določbe prava Unije upoštevati njeno besedilo ter njen kontekst in cilje, ki jih uresničuje ureditev, katere del je.

V zvezi z besedilom določb, na katere se nanašajo vprašanja za predhodno odločanje, je Sodišče ugotovilo, da medtem ko se člen 12(2)(d) Direktive o zlorabi trga nanaša na pooblastilo AMF, da „zahteva obstoječe zapise telefonskih pogovorov in zapise podatkov o klicanih številkah ter prejetih klicih“, člen 23(2)(g) in (h) Uredbe o zlorabi trga napotuje na pooblastilo tega organa, da zahteva, po eni strani, „[…] zapise podatkov o telefonskem in podatkovnem prometu, ki jih imajo investicijska podjetja, kreditne institucije ali finančne institucije“, in po drugi strani, „kolikor to dovoljuje nacionalno pravo, obstoječe zapise podatkov o telefonskem in podatkovnem prometu, ki jih ima telekomunikacijski operater“. Po presoji Sodišča je iz besedila teh določb nedvoumno razvidno, da te zgolj določajo meje pristojnosti AMF, da „zahteva“ podatke, ki jih imajo ti operaterji, kar ustreza dostopu do teh podatkov. Poleg tega sklicevanje na „obstoječe“ zapise, kot „jih imajo“ navedeni operaterji, kaže na to, da zakonodajalec Unije ni nameraval urediti možnosti nacionalnega zakonodajalca, da uvede obveznost hrambe takih zapisov. Po mnenju Sodišča je ta razlaga poleg tega podprta tako s kontekstom, v

[56] Direktiva 2003/6/ES Evropskega parlamenta in Sveta z dne 28. januarja 2003 o trgovanju z notranjimi informacijami in tržni manipulaciji (Zloraba trga) (UL, posebna izdaja v slovenščini, poglavje 6, zvezek 4, str. 367).

katerega se umeščajo navedene določbe, kot s cilji, ki jih uresničuje ureditev, katere del so te določbe.

Sodišče je v zvezi s kontekstom, v katerega spadajo določbe, na katere se nanašajo vprašanja za predhodno odločanje, ugotovilo, da je zakonodajalec Unije v skladu z upoštevnimi določbami Direktive o zlorabi trga in Uredbe o zlorabi trga[57] želel državam članicam naložiti, da sprejmejo potrebne ukrepe za zagotovitev, da imajo organi, pristojni na finančnem področju, na voljo vsa ustrezna orodja, pristojnosti in sredstva ter pooblastila za nadzor in preiskavo, ki so potrebna za zagotovitev učinkovitosti izvajanja njihovih nalog, pri čemer v teh določbah niso omenjene niti morebitne možnosti držav članic, da v ta namen v breme operaterjev storitev elektronskih komunikacij uvedejo splošno in neselektivno obveznost hrambe podatkov o prometu, niti pogoji, v katerih morajo operaterji te podatke shraniti za njihovo potencialno posredovanje pristojnim organom.

Glede ciljev, ki jim sledi zadevna ureditev, je Sodišče poudarilo, da tako iz Direktive o zlorabi trga kot iz Uredbe o zlorabi trga[58] izhaja, da je namen teh instrumentov zagotoviti integriteto finančnih trgov Unije in okrepiti zaupanje vlagateljev v te trge, pri čemer zaupanje temelji zlasti na tem, da bodo ti vlagatelji postavljeni v enakopraven položaj in zaščiteni pred nezakonito uporabo notranjih informacij. Cilj prepovedi trgovanja na podlagi notranjih informacij, ki je določen v navedenih instrumentih,[59] je tako zagotoviti enakost sopogodbenikov pri borzni transakciji, tako da se prepreči, da bi eden od njih, ki ima notranjo informacijo in je zato v ugodnejšem položaju v primerjavi z drugimi vlagatelji, od te informacije imel korist v škodo tistih, ki te informacije ne poznajo. Čeprav so v skladu z Uredbo o zlorabi trga[60] zapisi podatkov o povezavi bistven in včasih edini dokaz, ki omogoča odkritje in dokaz obstoja trgovanja na podlagi notranjih informacij ali tržne manipulacije, pa se ta uredba nanaša le na zapise „pri“ operaterjih storitev elektronskih komunikacij in na pooblastilo organa, pristojnega na finančnem področju, da od teh operaterjev „zahteva“ posredovanje „obstoječih“ podatkov. Tako iz tega besedila nikakor ne izhaja, da je zakonodajalec Unije tako želel državam članicam priznati pristojnost, da operaterjem elektronskih komunikacijskih storitev naložijo splošno obveznost hrambe podatkov. Iz tega sledi, da niti Direktiva o zlorabi trga niti Uredba o zlorabi trga ne moreta biti pravna podlaga za splošno obveznost hrambe zapisov podatkov o prometu, ki jih imajo operaterji elektronskih komunikacijskih storitev, za izvajanje pooblastil, podeljenih organu, pristojnemu za finančno področje, na podlagi teh aktov.

Dalje, Sodišče je opozorilo, da je Direktiva 2002/58 referenčni akt na področju hrambe in, splošneje, obdelave osebnih podatkov v sektorju elektronskih komunikacij, tako da razlaga, ki jo je Sodišče podalo glede te direktive, ureja tudi zapise podatkov o prometu,

57 Člen 12(1) Direktive o zlorabi trga in člen 23(3) Uredbe o zlorabi trga v povezavi z uvodno izjavo 62 te uredbe.

58 Uvodni izjavi 2 in 12 Direktive o zlorabi trga in člen 1 Uredbe o zlorabi trga v povezavi z uvodnima izjavama 2 in 24 te uredbe.

59 Člen 2(1) Direktive o zlorabi trga in člen 8(1) Uredbe o zlorabi trga.

60 Uvodna izjava 62 Uredbe o zlorabi trga.

ki jih hranijo operaterji elektronskih komunikacijskih storitev in katerih posredovanje od njih lahko zahtevajo organi, pristojni na finančnem področju, v smislu Direktive o zlorabi trga in Uredbe o zlorabi trga[61]. Presojo zakonitosti obdelave zapisov, ki jih imajo operaterji elektronskih komunikacijskih storitev,[62] je torej treba opraviti ob upoštevanju pogojev, določenih v Direktivi 2002/58, in razlage te direktive v sodni praksi Sodišča.

Sodišče je tako razsodilo, da Direktiva o zlorabi trga in Uredba o zlorabi trga v povezavi z Direktivo 2002/58 in ob upoštevanju Listine nasprotujeta zakonskim ukrepom, ki preventivno zaradi boja proti kaznivim dejanjem zlorabe trga, katerih del je trgovanje na podlagi notranjih informacij, določajo, da operaterji elektronskih komunikacijskih storitev začasno, vendar splošno in neselektivno hranijo podatke o prometu za eno leto od nastanka zapisa.

Nazadnje, Sodišče je potrdilo svojo sodno prakso, v skladu s katero pravo Unije nasprotuje temu, da nacionalno sodišče časovno omeji učinke ugotovitve neveljavnosti, ki jo mora v skladu z nacionalnim pravom podati glede nacionalnih določb, ki na eni strani operaterjem elektronskih komunikacijskih storitev nalagajo splošno in neselektivno hrambo podatkov o prometu, na drugi strani pa omogočajo posredovanje takih podatkov organu, pristojnemu za finančno področje, brez predhodnega dovoljenja sodišča ali neodvisnega upravnega organa, zaradi nezdružljivosti teh določb z Direktivo 2002/58 v povezavi z Listino. Ob tem je Sodišče opozorilo, da dopustnost dokazov, pridobljenih s tako hrambo, v skladu z načelom procesne avtonomije držav članic spada v nacionalno pravo, če se upoštevata zlasti načeli enakovrednosti in učinkovitosti. Zadnjenavedeno načelo nacionalnemu kazenskemu sodišču nalaga, da ne upošteva informacij in dokazov, ki so bili pridobljeni s splošno in neselektivno hrambo, ki ni združljiva s pravom Unije, če se zadevne osebe ne morejo učinkovito izjaviti glede teh informacij in teh dokazov, ki se nanašajo na področje, glede katerega sodišče nima strokovnega znanja, in lahko odločilno vplivajo na presojo dejstev.

Sodba Sodišča (občna seja) z dne 30. aprila 2024, La Quadrature du Net in drugi (Osebni podatki in boj proti ponarejanju) (C-470/21, EU:C:2024:370)

Sodišče, ki je zasedalo na občni seji, je v okviru odločanja o predlogu za predhodno odločanje, ki ga je predložil Conseil d'État (državni svet, Francija), razvilo svojo sodno prakso v zvezi z Direktivo 2002/58 tako, da je natančneje pojasnilo, prvič, pogoje, pod katerimi splošna hramba IP-naslovov, ki jo izvajajo ponudniki elektronskih komunikacijskih storitev, ne pomeni resnega posega v pravice do spoštovanja zasebnega življenja, varstva osebnih podatkov in svobode izražanja, zagotovljene z Listino[63], in drugič, možnost, da javni organ dostopi do nekaterih osebnih podatkov, ki se

61 Člen 11 Direktive o zlorabi trga in člen 22 Uredbe o zlorabi trga.
62 V smislu člena 12(2)(d) Direktive o zlorabi trga in člena 23(2)(g) in (h) Uredbe o zlorabi trga.
63 Členi 7, 8 in 11 Listine.

hranijo pod takimi pogoji, v okviru boja proti kršitvam pravic intelektualne lastnine, storjenim na spletu.

V obravnavani zadevi so štiri združenja pri Premier ministre (predsednik vlade, Francija) vložila predlog za razveljavitev odloka o avtomatizirani obdelavi osebnih podatkov[64]. Ker o tem predlogu ni bilo odločeno, so ta združenja pri Conseil d'État (državni svet) vložila tožbo za razveljavitev te zavrnitvene odločbe zaradi molka. Menila so, da ta odlok in določbe, ki so njegova pravna podlaga[65], niso v skladu s pravom Unije.

Haute Autorité pour la diffusion des œuvres et la protection des droits sur internet (visoka oblast za razširjanje del in varstvo pravic na spletu, v nadaljevanju: Hadopi) je na podlagi francoske zakonodaje dovoljen dostop do nekaterih podatkov, ki jih morajo hraniti ponudniki elektronskih komunikacijskih storitev, da lahko identificira osebe, odgovorne za kršitev avtorske ali sorodnih pravic. Ti podatki se nanašajo na istovetnost posameznika, na katerega se nanašajo osebni podatki, in ustrezajo njegovemu IP-naslovu, ki so ga predhodno pridobile organizacije imetnikov pravic. Ko je imetnik IP-naslova, uporabljenega za dejavnosti, ki pomenijo tako kršitev, identificiran, Hadopi začne tako imenovani postopek „postopnega odgovora". Konkretno je pooblaščena, da tej osebi pošlje dve priporočili, ki pomenita opozorili, in – če se dejavnosti nadaljujejo – dopis, v katerem jo obvesti, da se lahko njene dejavnosti kazensko preganjajo. Nazadnje ima pravico, da zadevo predloži državnemu tožilstvu zaradi kazenskega pregona te osebe.[66]

Conseil d'État je v tem okviru na Sodišče naslovil vprašanje glede razlage Direktive 2002/58 v povezavi z Listino.[67]

Na prvem mestu, Sodišče je v zvezi s hrambo podatkov o istovetnosti in ustrezajočih IP-naslovov poudarilo, da vsaka splošna in neselektivna hramba IP-naslovov ne pomeni nujno resnega posega v pravice do spoštovanja zasebnega življenja, varstva osebnih podatkov in svobode izražanja, zagotovljene v Listini.

Obveznost zagotavljanja take hrambe je lahko utemeljena s ciljem boja proti kaznivim dejanjem na splošno, če je dejansko izključena možnost resnega posega v zasebno življenje zadevne osebe zaradi te hrambe, ker bi – med drugim s povezovanjem teh IP-naslovov z vsemi podatki o prometu ali lokaciji – lahko prišlo do natančnih ugotovitev o tej osebi.

---

64 Décret no 2010-236, du 5 mars 2010, relatif au traitement automatisé de données à caractère personnel autorisé par l'article L. 331-29 du code de la propriété intellectuelle dénommé „Système de gestion des mesures pour la protection des œuvres sur internet" (odlok št. 2010-236 z dne 5. marca 2010 o avtomatizirani obdelavi osebnih podatkov, ki je dovoljena s členom L. 331-29 zakonika o intelektualni lastnini in ki je imenovana „Sistem upravljanja ukrepov za varstvo del na spletu") (JORF št. 56 z dne 7. marca 2010, besedilo št. 19), kakor je bil spremenjen z décret no 2017-924, du 6 mai 2017, relatif à la gestion des droits d'auteur et des droits voisins par un organisme de gestion de droits et modifiant le code de la propriété intellectuelle (odlok št. 2017-924 z dne 6. maja 2017 o upravljanju avtorske in sorodnih pravic s strani organizacije za upravljanje pravic in o spremembi zakonika o intelektualni lastnini) (JORF št. 109 z dne 10. maja 2017, besedilo št. 176).

65 Zlasti člen L. 331-21, odstavki od prvega do petega, code de la propriété intellectuelle (zakonik o intelektualni lastnini).

66 Hadopi je bila s 1. januarjem 2022 združena z drugim neodvisnim javnim organom, Conseil supérieur de l'audiovisuel (višji svet za avdiovizualne medije, v nadaljevanju: CSA), v Autorité de régulation de la communication audiovisuelle et numérique (organ za regulacijo avdiovizualne in digitalne komunikacije, v nadaljevanju: ARCOM). Vendar je postopek postopnega odgovora v bistvu ostal nespremenjen.

67 Člen 15(1) Direktive 2002/58.

Zato se mora država članica, ki namerava ponudnikom elektronskih komunikacijskih storitev naložiti tako obveznost, prepričati, da je s podrobnimi pravili o hrambi teh podatkov zagotovljeno, da je izključena vsakršna možnost, da bi prišlo do natančnih ugotovitev o zasebnem življenju zadevnih oseb.

Sodišče je pojasnilo, da se morajo podrobna pravila o hrambi nanašati na samo strukturo hrambe, ki se mora v bistvu izvajati tako, da je zagotovljena dejansko neprepustna ločitev različnih kategorij shranjenih podatkov. Z nacionalnimi pravili o teh podrobnih pravilih je treba zagotoviti, da je vsaka kategorija podatkov, vključno s podatki o istovetnosti in IP-naslovi, shranjena povsem ločeno od preostalih kategorij shranjenih podatkov in da je ta ločitev dejansko neprepustna, in sicer z uporabo varnega in zanesljivega računalniškega sistema. Poleg tega, če je z navedenimi pravili določena možnost povezovanja shranjenih IP-naslovov z istovetnostjo posameznika, na katerega se nanašajo osebni podatki, se lahko s temi pravili tako povezovanje dopusti le z uporabo učinkovitega tehničnega postopka, s katerim se ne ogrozi neprepustna ločenost teh kategorij podatkov. Zanesljivost te ločitve mora biti predmet rednega nadzora, ki ga opravi neodvisen javni organ. Če so v veljavni nacionalni zakonodaji določene take stroge zahteve, posega, ki nastane s to hrambo IP-naslovov, ni mogoče opredeliti kot „resnega“.

Sodišče je zato sklenilo, da v primeru zakonodajnega ukrepa, s katerim se zagotovi, da z nikakršnim povezovanjem podatkov ne bo mogoče priti do natančnih ugotovitev o zasebnem življenju posameznikov, katerih podatki so shranjeni, Direktiva 2002/58 ne nasprotuje temu, da zadevna država članica zaradi uresničevanja cilja boja proti kaznivim dejanjem na splošno naloži obveznost splošne in neselektivne hrambe IP-naslovov za obdobje, ki ne presega nujno potrebnega.

Na drugem mestu, Sodišče je v zvezi z dostopom do podatkov o istovetnosti, ki ustrezajo IP-naslovom, potrdilo, da Direktiva 2002/58 v povezavi z Listino načeloma ne nasprotuje nacionalni ureditvi, ki javnemu organu dopušča dostop do teh podatkov, ki jih ločeno in dejansko neprepustno hranijo ponudniki elektronskih komunikacijskih storitev, zgolj zato, da lahko ta organ identificira imetnike teh naslovov, za katere se sumi, da so odgovorni za kršitve avtorske in sorodnih pravic na spletu, in po potrebi zoper njih sprejme ukrepe. V takem primeru mora biti v nacionalni zakonodaji uslužbencem, ki imajo tak dostop, prepovedano, prvič, da v kakršni koli obliki razkrijejo informacije o vsebini datotek, do katerih so dostopali ti imetniki, razen zaradi predložitve zadeve državnemu tožilstvu, drugič, da sledijo brskanju, ki so ga ti imetniki opravili, in tretjič, da te IP-naslove uporabljajo za druge namene, kot je sprejetje teh ukrepov.

Sodišče je v tem okviru med drugim spomnilo, da čeprav sta svoboda izražanja in zaupnost osebnih podatkov osrednja preudarka, ti temeljni pravici vseeno nista absolutni. V okviru tehtanja med zadevnimi pravicami in interesi se morajo ti namreč včasih umakniti drugim temeljnim pravicam in nujnim razlogom v splošnem interesu, kot so varovanje javnega reda, preprečevanje kaznivih dejanj ali varstvo pravic in svoboščin drugih. To velja zlasti v primeru, kadar prevlada navedenih osrednjih

preudarkov ovira učinkovitost kazenske preiskave, zlasti tako, da onemogoča ali pretirano otežuje dejansko identifikacijo storilca kaznivega dejanja in naložitev sankcije navedenemu storilcu.

Sodišče se je v tem okviru sklicevalo na svojo sodno prakso, v skladu s katero – v okviru boja proti kaznivim ravnanjem, s katerimi se kršijo avtorska ali sorodne pravice na spletu – okoliščina, da je dostop do IP-naslova lahko edino preiskovalno sredstvo, ki omogoča dejansko identifikacijo zadevne osebe, kaže na to, da sta hramba teh podatkov in dostop do njih nujno potrebna za uresničitev zastavljenega cilja in sta torej v skladu z zahtevo po sorazmernosti. Če se tak dostop ne bi dopustil, bi to pomenilo dejansko tveganje sistemske nekaznovanosti kaznivih ravnanj, storjenih na spletu ali katerih storitev ali priprava sta olajšani s posebnimi značilnostmi spleta. Obstoj takega tveganja je namreč v okviru tehtanja različnih zadevnih pravic in interesov upoštevna okoliščina pri presoji, ali je poseg v pravice do spoštovanja zasebnega življenja, varstva osebnih podatkov in svobode izražanja sorazmeren ukrep glede na cilj boja proti kaznivim dejanjem.

Na tretjem mestu, Sodišče je v okviru odločanja o vprašanju, ali mora biti dostop javnega organa do podatkov o istovetnosti, ki ustrezajo IP-naslovu, predmet predhodnega nadzora, ki ga opravi sodišče ali neodvisen upravni organ, menilo, da je tak nadzor potreben, kadar v okviru nacionalne ureditve pri tem dostopu obstaja nevarnost resnega posega v temeljne pravice posameznika, na katerega se nanašajo osebni podatki, v smislu, da bi lahko javni organ na podlagi tega dostopa prišel do natančnih ugotovitev o zasebnem življenju tega posameznika in, odvisno od primera, izdelal njegov podroben profil. Nasprotno se ta zahteva po predhodnem nadzoru ne uporablja, kadar posega v zadevne temeljne pravice ni mogoče šteti za resnega.

Sodišče je v zvezi s tem pojasnilo, da se v primeru ukrepa hrambe, s katerim je zagotovljena dejansko neprepustna ločitev različnih kategorij shranjenih podatkov, za dostop javnega organa do podatkov o istovetnosti, ki ustrezajo tako shranjenim IP-naslovom, načeloma ne zahteva predhodni nadzor. Tak dostop zgolj za identifikacijo imetnika IP-naslova namreč praviloma ne pomeni resnega posega v zgoraj navedene pravice.

Vendar Sodišče ni izključilo možnosti, da v neobičajnih položajih obstaja nevarnost, da bi lahko javni organ v okviru postopka, kot je postopek postopnega odgovora iz zadeve v glavni stvari, prišel do natančnih ugotovitev o zasebnem življenju zadevne osebe, med drugim kadar ta oseba izvaja dejavnosti, s katerimi redno ali obsežno krši avtorsko ali sorodne pravice na omrežjih enakovrednih partnerjev, v povezavi z določenimi vrstami varovanih del, ki lahko razkrijejo informacije – v nekaterih primerih občutljive – o zasebnem življenju te osebe.

V obravnavanem primeru je lahko imetnik IP-naslova še posebej izpostavljen taki nevarnosti, če se mora javni organ odločiti, ali bo zadevo predložil državnemu tožilstvu zaradi pregona tega imetnika. Verjetno je namreč, da se intenzivnost posega v pravico

do spoštovanja zasebnega življenja s tem, da postopek postopnega odgovora, ki je večfazni postopek, prehaja v svoje različne faze, povečuje. Pristojni organ lahko na podlagi dostopa do vseh podatkov, ki se nanašajo na zadevno osebo in ki se zberejo v različnih fazah tega postopka, pride do natančnih ugotovitev o njenem zasebnem življenju. Zato mora biti v nacionalni ureditvi določen predhodni nadzor, ki se mora opraviti, preden lahko javni organ podatke o istovetnosti poveže s tako celoto podatkov in preden se morda pošlje uradno obvestilo, v katerem je ugotovljeno, da je ta oseba storila dejanja, ki jih je mogoče kazensko preganjati. S tem nadzorom mora biti poleg tega ohranjena učinkovitost postopka postopnega odgovora, da se zlasti omogoči opredelitev primerov morebitnega vnovičnega ponavljanja zadevnega kršitvenega ravnanja. Zato mora biti ta postopek organiziran in strukturiran tako, da osebe, ki so pri pristojnemu javnemu organu pooblaščene za preiskavo dejanja, podatkov o istovetnosti osebe, ki ustrezajo IP-naslovom, ki so bili predhodno pridobljeni na spletu, ne morejo samodejno povezati z datotekami, v katerih so elementi, s katerimi ta organ že razpolaga in na podlagi katerih lahko pride do natančnih ugotovitev o zasebnem življenju zadevne osebe.

Poleg tega je Sodišče glede predmeta predhodnega nadzora ugotovilo, da v primerih, v katerih je zadevna oseba osumljena storitve kršitve, ki spada pod kazniva ravnanja na splošno, mora sodišče ali neodvisen upravni organ, ki je pristojen za ta nadzor, zavrniti dostop, če bi lahko javni organ na njegovi podlagi prišel do natančnih ugotovitev o zasebnem življenju navedene osebe. Vendar pa bi moral biti tudi dostop, na podlagi katerega je mogoče priti do takih natančnih ugotovitev, dopusten v primerih, v katerih je zadevna oseba osumljena storitve kaznivega dejanja, za katero zadevna država članica šteje, da spada na področje hudega kriminala.

Sodišče je pojasnilo tudi, da predhodni nadzor nikakor ne sme biti popolnoma avtomatiziran, saj je treba v primeru kazenske preiskave v okviru takega nadzora tehtati med interesi, povezanimi z bojem proti kriminalu, na eni strani ter spoštovanjem zasebnega življenja in varstva osebnih podatkov na drugi. Tako tehtanje pa mora opraviti fizična oseba, kar je še toliko bolj potrebno v primeru, v katerem je pravica do zasebnega življenja zaradi avtomatiziranosti in velikega obsega zadevne obdelave podatkov ogrožena.

Zato je Sodišče sklenilo, da mora biti možnost, da osebe, ki so pristojne za preverjanje dejstev pri javnem organu, podatke o istovetnosti neke osebe, ki ustrezajo IP-naslovu, povežejo z datotekami, v katerih so elementi, iz katerih se lahko ugotovijo naslovi varovanih del, katerih dajanje na voljo na spletu je bil razlog, da so organizacije imetnikov pravic zbrale njihove IP-naslove, v primerih, v katerih ista oseba ponovi dejavnost, s katero se kršijo avtorska pravica ali sorodne pravice, predmet nadzora, ki ga opravi sodišče ali neodvisen upravni organ. Ta nadzor ne more biti povsem avtomatiziran in ga je treba opraviti pred takim povezovanjem, saj v takih primerih na podlagi takega povezovanja lahko pride do natančnih ugotovitev o zasebnem življenju

navedene osebe, katere IP-naslov je bil uporabljen za dejavnosti, s katerimi bi se lahko kršile avtorska pravica ali sorodne pravice.

Na četrtem in zadnjem mestu, Sodišče je ugotovilo, da mora biti sistem obdelave podatkov, ki ga uporablja javni organ, predmet rednega nadzora, ki ga opravlja neodvisen organ, ki je v razmerju do tega javnega organa tretja oseba. V okviru tega nadzora se preveri celovitost sistema, vključno z učinkovitimi jamstvi pred tveganji nezakonitega dostopa do teh podatkov ali njihove nezakonite uporabe oziroma dostopa in uporabe, ki bi pomenila zlorabo, kot tudi njegova učinkovitost in zanesljivost za odkrivanje kršitvenih ravnanj.

Sodišče je v tem okviru ugotovilo, da lahko v obravnavanem primeru avtomatizirana obdelava, ki jo opravi javni organ na podlagi informacij o ponaredkih, ki so jih ugotovile organizacije imetnikov pravic, vključuje nekaj lažnih pozitivnih primerov in zlasti nevarnost, da se bodo tretje osebe nezakonito ali z namenom zlorabe polastile morda zelo visokega števila osebnih podatkov, zaradi česar je potreben ta nadzor. Dodalo je tudi, da mora biti ta obdelava v skladu s posebnimi pravili o varstvu podatkov, določenih v Direktivi 2016/680. Čeprav javni organ v obravnavani zadevi v okviru postopka postopnega odgovora nima pristojnosti za odločanje, ga je treba šteti za „javni organ“, ki sodeluje pri preprečevanju in odkrivanju kaznivih dejanj, in torej spada na področje uporabe te direktive. Zato morajo biti osebam, ki so v takem postopku, zagotovljena vsa materialna in postopkovna jamstva, določena z Direktivo 2016/680, predložitveno sodišče pa mora preveriti, ali so ta jamstva določena v nacionalni zakonodaji.

2. Obdelava osebnih podatkov v kazenskih zadevah

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 ta 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[68] 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 tega, da se je skliceval 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.[69]

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.

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 na seznam iskanih oseb države članice, pomeni „obdelavo“, ki spada na področje uporabe Direktive 2016/680.[70] 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.[71] Ta

[68] 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).

[69] 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).

[70] Glej člen 2(1) in člen 3, točka 2, Direktive 2016/680.

[71] Glej člen 4(1)(b) in člen 8(1) Direktive 2016/680.

obdelava, ki jo opravljajo organi držav članic, se poleg tega lahko izkaže za nepogrešljivo ravno zato, da se preveri, ali se navedeno načelo uporablja.

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.[72]

Kadar pa se načelo *ne bis in idem* uporablja, ni več potrebno, da se osebni podatki, navedeni v Interpolovi rdeči mednarodni tiralici, vnesejo na 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 zadevna oseba zaradi načela *ne bis in idem* v državi članici ali državi pogodbenici ne sme več biti preganjana za ista dejanja.

Sodba z dne 21. junija 2022 (veliki senat), Ligue des droits humains (C-817/19, EU:C:2022:491)

Sodišče je v tej sodbi (glej tudi razdelek I.1., naslovljen „Skladnost sekundarnega prava Unije s pravico do varstva osebnih podatkov“) po tem, ko je ugotovilo veljavnost Direktive PNR, podalo dodatna pojasnila glede razlage nekaterih določb te direktive.[73]

Prvič, Sodišče je navedlo, da so v tej direktivi cilji obdelave podatkov PNR našteti izčrpno. Zato ta direktiva nasprotuje nacionalni zakonodaji, ki dovoljuje obdelavo podatkov PNR za namene, ki niso boj proti terorističnim in hudim kaznivim dejanjem. Tako se lahko z nacionalno zakonodajo, ki poleg tega kot namen obdelave podatkov PNR dopušča spremljanje dejavnosti, ki jih izvajajo obveščevalno-varnostne službe, krši izčrpnost tega seznama. Prav tako sistema, vzpostavljenega z Direktivo o PNR, ni mogoče določiti za izboljšanje mejnih kontrol in boj proti nezakonitemu priseljevanju. Iz tega tudi sledi, da se podatki PNR ne smejo hraniti v enotni podatkovni zbirki, ki bi jo bilo mogoče uporabljati za namene Direktive o PNR in za druge namene.

Drugič, Sodišče je pojasnilo pojem neodvisnega nacionalnega organa, ki je pristojen za preverjanje, ali so izpolnjeni pogoji za razkritje podatkov PNR za namene njihovega naknadnega ocenjevanja in za odobritev takega razkritja. Natančneje, organa, ki je ustanovljen kot enota za informacije o potnikih, ni mogoče opredeliti kot takega, ker v

[72] Glej člen 1(1) in člen 8(1) Direktive 2016/680.

[73] Natančneje, člen 2 („Uporaba [Direktive] za lete znotraj EU“), člen 6 („Obdelava podatkov PNR“) in člen 12 („Čas hrambe podatkov in depersonalizacija“) Direktive o PNR.

razmerju do organa, ki prosi za dostop do podatkov, ni tretja oseba. Ker so namreč člani njegovega osebja lahko uslužbenci, ki jih napotijo organi, ki so upravičeni do zaprosila za tak dostop, je razvidno, da je enota za informacije o potnikih nujno povezana s temi organi. Zato Direktiva o PNR nasprotuje nacionalni zakonodaji, v skladu s katero je organ, ustanovljen kot enota za informacije o potnikih, tudi pristojni nacionalni organ, ki je pooblaščen za odobritev razkritja podatkov PNR po izteku šestih mesecev od prenosa teh podatkov enoti za informacije o potnikih.

Tretjič, Sodišče je v zvezi z obdobjem hrambe podatkov PNR razsodilo, da člen 12 Direktive o PNR v povezavi s členoma 7 in 8 ter členom 52(1) Listine nasprotuje nacionalni zakonodaji, ki določa splošno petletno obdobje hrambe teh podatkov, ki se uporablja brez razlikovanja za vse letalske potnike.

Po mnenju Sodišča namreč ni razvidno, da bi bila hramba podatkov PNR po izteku začetnega šestmesečnega obdobja hrambe omejena na tisto, kar je nujno potrebno v zvezi z letalskimi potniki, za katere niti predhodno ocenjevanje niti morebitna preverjanja, opravljena v začetnem šestmesečnem obdobju hrambe, niti nobena druga okoliščina niso pokazali na obstoj objektivnih elementov – kot je to, da v okviru predhodnega ocenjevanja iz podatkov PNR o zadevnih potnikih izhaja preverjen zadetek – ki bi lahko dokazovali tveganje v zvezi s terorističnimi ali hudimi kaznivimi dejanji, ki so objektivno, vsaj posredno, povezana z letalskim prevozom teh potnikov. Sodišče pa je na drugi strani menilo, da ni razvidno, da bi hramba podatkov PNR o vseh letalskih potnikih, za katere velja sistem, vzpostavljen s to direktivo, med začetnim šestmesečnim obdobjem načeloma presegala meje tega, kar je nujno potrebno.

Četrtič, Sodišče je dalo napotke v zvezi z morebitno uporabo Direktive o PNR za namene boja proti terorističnim in hudim kaznivim dejanjem za druge načine prevoza, s katerimi se v Uniji prevažajo potniki. Ta direktiva v povezavi s členom 3(2) PEU, členom 67(2) PDEU in členom 45 Listine namreč nasprotuje sistemu prenosa in obdelave podatkov PNR o vseh prevozih, opravljenih z drugimi prevoznimi sredstvi znotraj Unije, ob neobstoju resnične in sedanje ali predvidljive teroristične grožnje, s katero se spopada zadevna država članica. V takem položaju mora biti uporaba sistema, vzpostavljenega z Direktivo o PNR, tako kot za lete znotraj EU omejena na podatke PNR o prevozih, ki se med drugim nanašajo na nekatere povezave, določene potovalne načrte ali celo na nekatere železniške postaje ali nekatera pristanišča, za katera obstajajo indici, ki lahko upravičijo to uporabo. Zadevna država članica mora izbrati prevoze, za katere obstajajo taki indici, in to uporabo redno pregledovati glede na razvoj okoliščin, ki so utemeljevale njihovo izbiro.

IV. Prenos osebnih podatkov v tretje države

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

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.

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 dostopni osebam iz tretjih držav, ki imajo tehnična sredstva za dostop do njih.

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

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[74] ugotovila, da Združene države v okviru sistema „varnega pristana" (angleško „safe harbour")[75], 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

[74] 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).

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

ugotavljanje 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 v povezavi z Listino, 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.

Sodišče je poleg tega ugotovilo, da člen 3 Odločbe 2000/520 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. Sodišče je nazadnje ugotovilo, da neveljavnost členov 1 in 3 Odločbe 2002/520 vpliva na veljavnost te odločbe v celoti.

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

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. 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. 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.

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 in, natančneje, 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 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 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 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.

Prvič, Sodišče je ugotovilo, da tako prenos podatkov 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.

Poleg tega je poudarilo, da tudi če se zdi, da nekateri podatki 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).

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.

Drugič, Sodišče je menilo, da nadaljnja hramba podatkov 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 PNR in ciljem predvidenega sporazuma, ki bi upravičevala hrambo teh podatkov. Vendar je dopustno hraniti podatke 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.

Tretjič, Sodišče je ugotovilo, da temeljna pravica do spoštovanja zasebnega življenja, določena v členu 7 Listine 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 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.

Sodba z dne 16. julija 2020 (veliki senat), Facebook Ireland in Schrems (C-311/18, EU:C:2020:559)

SUVP 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.[76] 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.[77] Poleg tega SUVP natančno določa pogoje, pod katerimi je tak prenos mogoč, če ni bil sprejet sklep o ustreznosti ali niso bili zagotovljeni ustrezni zaščitni ukrepi.[78]

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 zavrnjena med drugim zato, ker je Komisija v Odločbi 2000/520[79] ugotovila, da Združene države zagotavljajo ustrezno raven varstva. Sodišče je s sodbo z dne 6. oktobra 2015 na podlagi vprašanja za predhodno

[76] Člen 45 SUVP.

[77] Člen 46(1) in (2)(c) SUVP.

[78] Člen 49 SUVP.

[79] Odločba Komisije z dne 26. julija 2000 po Direktivi 95/46/ES 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).

odločanje, ki mu ga je predložilo High Court (višje sodišče, Irska), to odločbo razglasilo za neveljavno (v nadaljevanju: sodba Schrems I)[80].

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.[81] 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[82].

Predložitveno sodišče je v predlogu za sprejetje predhodne odločbe Sodišče spraševalo o uporabi SUVP 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.

Sodišče je najprej ugotovilo, da se pravo Unije, med drugim tudi SUVP, 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.

Glede ravni varstva, ki se zahteva pri takem prenosu, je Sodišče razsodilo, da je treba zahteve, ki jih v zvezi s tem vsebuje SUVP ter se nanašajo na 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

[80] Sodba Sodišča z dne 6. oktobra 2015, Schrems (C-362/14, *EU:C:2015:650*).

[81] 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).

[82] 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).

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.

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.

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 navedeni sklep 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.

Nazadnje je Sodišče preučilo veljavnost Sklepa 2016/1250 glede na zahteve, ki izhajajo iz SUVP v povezavi z določbami 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.

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.

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 tudi razdelka II.1. in II.3., naslovljena „Področje uporabe splošne ureditve“ in „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 je pojasnilo, 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.

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. Če je torej po tem, ko je zadevna oseba vložila zahtevo, ugotovljeno, da zdaj to, da so na seznam vključene te povezave, ni združljivo s to direktivo, je treba informacije in zadevne povezave navedenega seznama izbrisati. 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.

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.

2. Obdelava osebnih podatkov in pravice intelektualne lastnine

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

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 zadnjenavedena družba 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),[83] Direktiva 2001/29/ES o usklajevanju določenih vidikov avtorske in sorodnih pravic v informacijski družbi,[84] Direktiva 2004/48/ES o uveljavljanju pravic intelektualne lastnine[85] 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 navedenih 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.

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

[83] 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).

[84] 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).

[85] 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).

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 (vrhovno sodišče), 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 razlagati nacionalno pravo v skladu s temi direktivami in 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.

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.

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.

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, EU:C:2019:773)

Sodišče, ki je zasedalo v velikem senatu, 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 (nacionalna komisija za informatiko in svoboščine, CNIL, Francija) zavrnila, da bi družbo Google pozvala, naj izbriše 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 prepričanja ali članstvo v sindikatu, in obdelava podatkov v zvezi z zdravjem ali spolnim življenjem – ob upoštevanju nekaterih izjem in odstopanj – prepovedana.[86] 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.[87]

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 hud poseg v temeljni pravici do spoštovanja zasebnega življenja in varstva osebnih podatkov.

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.

Drugič, Sodišče je štelo, da mora upravljavec iskalnika, kadar prejme zahtevo za odstranitev povezav v zvezi z občutljivimi podatki, tej zahtevi načeloma in ob

[86] Člen 8(1) Direktive 95/46 in člen 9(1) Uredbe 2016/679.
[87] Člen 8(5) Direktive 95/46 in člen 10 Uredbe 2016/679.

upoštevanju določenih izjem ugoditi. Glede teh izjem lahko upravljavec taki zahtevi ne ugodi zlasti, kadar ugotovi, da povezave vodijo do podatkov, ki jih je zadevna oseba očitno javno objavila,[88] 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.[89]

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.

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.

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

Commission nationale de l'informatique et des libertés (nacionalna komisija za informatiko in svoboščine, CNIL, 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,

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

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.[90]

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[91] 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.

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.

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 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

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

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

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.

Sodba z dne 8. decembra 2022 (veliki senat), Google (Odstranitev povezav do domnevno netočne vsebine) (C-460/20, EU:C:2022:962)

Tožeči stranki v postopku v glavni stvari, TU, ki zaseda odgovorne položaje in ima deleže v različnih družbah, in RE, ki je bila njegova partnerka in do maja 2015 prokuristka ene od teh družb, sta bili predmet treh člankov, ki jih je leta 2015 na spletnem mestu objavila družba G LLC, ki je izdajatelj tega spletnega mesta. V teh člankih, od katerih je bil eden ilustriran s štirimi fotografijami, ki so upodabljale tožeči stranki in ki so kazale na to, da ti živita luksuzno življenje, je bil kritično predstavljen naložbeni model več njunih družb. Dostop do teh člankov je bil mogoč tako, da so se v iskalnik, ki ga upravlja družba Google LLC (v nadaljevanju: Google), vnesla imena in priimki tožečih strank, tako ločeno kot v kombinaciji z nekaterimi imeni družb. Seznam zadetkov je napotoval na te članke, in sicer prek povezave, in na fotografije, prikazane v obliki predoglednih sličic („thumbnails“).

Tožeči stranki v postopku v glavni stvari sta od družbe Google kot upravljavca obdelave osebnih podatkov, ki se izvaja z njenim iskalnikom, zahtevali, prvič, naj s seznama zadetkov iskanja odstrani povezave do zadevnih člankov, ker naj bi ti vsebovali netočne trditve in obrekljiva mnenja, in drugič, naj s seznama zadetkov iskanja odstrani predogledne sličice. Družba Google tej zahtevi ni ugodila.

Ker tožeči stranki v postopku v glavni stvari nista uspeli niti na prvi stopnji niti v pritožbenem postopku, sta pri Bundesgerichtshof (zvezno vrhovno sodišče, Nemčija) vložili revizijo, v okviru katere je Bundesgerichtshof pri Sodišču vložilo predlog za sprejetje predhodne odločbe glede razlage SUVP in Direktive 95/46.[92]

Sodišče je s sodbo, izdano v velikem senatu, razvilo svojo sodno prakso glede pogojev, ki se uporabljajo za zahteve za odstranitev povezav, naslovljene na upravljavca iskalnika, na podlagi pravil glede varstva osebnih podatkov. Zlasti je preučilo, po eni strani, obseg obveznosti in odgovornosti, ki jih ima upravljavec iskalnika pri obravnavi zahteve za odstranitev povezav, ki temelji na domnevni netočnosti informacij v vsebini, uvrščeni na seznam zadetkov, in po drugi strani dokazno breme, ki ga ima posameznik, na katerega se nanašajo osebni podatki, glede te netočnosti. Poleg tega se je izreklo o tem, ali je treba za preučitev zahteve za izbris fotografij, prikazanih v obliki predoglednih sličic na seznamu rezultatov slikovnega iskanja, upoštevati prvotni kontekst objave teh fotografij na spletu.

[92] Člen 17(3)(a) SUVP ter člen 12(b) in člen 14, prvi odstavek, (a), Direktive 95/46.

Na prvem mestu, Sodišče je razsodilo, da v okviru tehtanja med pravicama do spoštovanja zasebnega življenja in varstva osebnih podatkov na eni strani in pravico do svobode izražanja in obveščanja[93] na drugi strani za namene obravnave zahteve za odstranitev povezav, naslovljene na upravljavca iskalnika, katere cilj je, da se s seznama zadetkov iskanja odstrani povezava, ki vodi do vsebine, ki zajema domnevno netočne informacije, za to odstranitev povezav ne velja pogoj, da je bilo vprašanje točnosti vsebine, uvrščene na seznam zadetkov, vsaj začasno, rešeno v okviru tožbe, ki jo je vlagatelj zahteve vložil proti ponudniku vsebine.

Sodišče je najprej zaradi preučitve, pod katerimi pogoji mora upravljavec iskalnika ugoditi zahtevi za odstranitev povezav in torej s seznama zadetkov, ki se prikaže po iskanju, opravljenem na podlagi imena zadevne osebe, odstraniti povezavo do spletne strani, na kateri so trditve, za katere ta oseba meni, da so netočne, zlasti opozorilo:

• ker lahko dejavnost spletnega iskalnika pomembno in dodatno – poleg dejavnosti izdajateljev spletnih mest – vpliva na temeljni pravici do spoštovanja zasebnega življenja in varstva osebnih podatkov, mora upravljavec iskalnika kot oseba, ki določa namene in sredstva te dejavnosti, v okviru svojih odgovornosti, pristojnosti in zmožnosti zagotoviti, da imajo lahko jamstva, ki jih določata Direktiva 95/46 in SUVP, polni učinek in da se lahko zadevnim osebam dejansko zagotovi učinkovito in celovito varstvo;

• upravljavec iskalnika mora, kadar prejme zahtevo za odstranitev povezav, preveriti, ali je vključitev povezave do zadevne spletne strani na seznam zadetkov potrebna za uresničevanje pravice do svobode obveščanja spletnih uporabnikov, ki so potencialno zainteresirani za dostop do te spletne strani s takim iskanjem, varovane s pravico do svobode izražanja in obveščanja;

• SUVP izrecno določa zahtevo po tehtanju med, na eni strani, temeljnima pravicama do spoštovanja zasebnega življenja in varstva osebnih podatkov ter, na drugi strani, temeljno pravico do svobode obveščanja.

Sodišče je najprej poudarilo, da čeprav pravici do spoštovanja zasebnega življenja in varstva osebnih podatkov zadevne osebe na splošno prevladata nad legitimnim interesom spletnih uporabnikov za dostop do zadevne informacije, je to ravnotežje lahko odvisno od upoštevnih okoliščin vsakega primera, zlasti narave te informacije, od tega, kako občutljiva je za zasebno življenje zadevne osebe, in od interesa javnosti, da razpolaga s to informacijo, ki je lahko med drugim odvisen od vloge, ki jo ima ta oseba v javnem življenju.

Vprašanje točnosti ali netočnosti vsebine, uvrščene na seznam zadetkov, je prav tako upošteven element pri tej presoji. Tako lahko v nekaterih okoliščinah pravica do obveščanja spletnih uporabnikov in svoboda izražanja ponudnika vsebine prevladata nad pravico do varstva zasebnega življenja in do varstva osebnih podatkov, zlasti kadar ima posameznik, na katerega se nanašajo osebni podatki, vlogo v javnem življenju.

[93] Temeljne pravice, ki so določene v členih 7, 8 in 11 Listine.

Vendar se to razmerje obrne, kadar se vsaj del informacij, na katere se nanaša zahteva za odstranitev povezav, ki glede na celotno vsebino niso manj pomembne, izkaže za netočen. V takem primeru namreč pravice do obveščanja in pravice do obveščenosti ni mogoče upoštevati, saj ne moreta vključevati pravice do razširjanja takih informacij in do dostopa do njih.

Dalje, glede, na eni strani, obveznosti v zvezi z dokazovanjem točnosti oziroma netočnosti informacij iz vsebine, uvrščene na seznam zadetkov, je Sodišče pojasnilo, da mora oseba, ki zahteva odstranitev povezav zaradi netočnosti takih informacij, dokazati očitno netočnost teh informacij ali vsaj dela teh informacij, ki glede na celotno vsebino niso manj pomembne. Vendar mora – za preprečitev tega, da bi se tej osebi naložilo preveliko breme, ki bi lahko škodilo polnemu učinku pravice do odstranitve povezav – ta zgolj predložiti dokaze, ki jih je mogoče glede na okoliščine posameznega primera razumno zahtevati od nje. Tej osebi načeloma ni mogoče naložiti, naj že v predhodnem postopku v utemeljitev svoje zahteve za odstranitev povezav predloži sodno odločbo, ki je bila izdana zoper izdajatelja zadevnega spletnega mesta, čeprav v obliki odločbe, sprejete v postopku za izdajo začasne odredbe.

Po drugi strani je Sodišče glede obveznosti in odgovornosti, ki jih ima upravljavec iskalnika, poudarilo, da se mora ta, da bi preveril, ali je lahko neka vsebina še naprej vključena na seznam zadetkov iskanja, ki se opravi z njegovim iskalnikom, po zahtevi za odstranitev povezav opreti na vse prisotne pravice in interese ter na vse okoliščine obravnavanega primera. Vendar ta upravljavec ne more biti zavezan k temu, da poizveduje za dejstvi in v ta namen organizira kontradiktorno razpravo s ponudnikom vsebin, da bi pridobil manjkajoče podatke v zvezi s točnostjo vsebine, uvrščene na seznam zadetkov. Obveznost, da prispeva k ugotovitvi točnosti oziroma netočnosti vsebine, uvrščene na seznam zadetkov, bi temu upravljavcu naložila breme, ki presega tisto, kar je od njega mogoče razumno pričakovati glede na njegove odgovornosti, pristojnosti in zmožnosti. Ta rešitev bi tako pomenila resno tveganje, da se povezave do vsebin, ki zadovoljujejo legitimno in prevladujočo potrebo javnosti po obveščanju, odstranijo in da jih je tako težko najti na spletu. Tako bi obstajala resnična nevarnost odvračilnega učinka glede uresničevanja svobode izražanja in obveščanja, če bi tak upravljavec take povezave skoraj sistematično odstranil, da bi se izognil temu, da nosi breme poizvedovanja za upoštevnimi dejstvi, zaradi ugotavljanja točnosti oziroma netočnosti vsebine, uvrščene na seznam zadetkov.

Zato mora, kadar oseba, ki je vložila zahtevo za odstranitev povezav, predloži dokaze, ki dokazujejo očitno netočnost informacij iz vsebine, uvrščene na seznam zadetkov, ali vsaj dela teh informacij, ki glede na celotno vsebino ni manj pomemben, upravljavec iskalnika tej zahtevi za odstranitev povezav ugoditi. Enako velja, kadar ta vlagatelj predloži sodno odločbo, sprejeto proti izdajatelju spletne strani, ki temelji na ugotovitvi, da so informacije iz vsebine, uvrščene na seznam zadetkov, ki glede na celotno vsebino niso manj pomembne, vsaj na prvi pogled netočne. Če pa glede na dokaze, ki jih je predložil vlagatelj, ni očitno, da so take informacije netočne, upravljavcu iskalnika ob

neobstoju take sodne odločbe ni treba ugoditi zahtevi za odstranitev povezav. Kadar lahko zadevne informacije prispevajo k razpravi v splošnem interesu, je treba glede na vse druge okoliščine konkretnega primera poseben pomen pripisati pravici do svobode izražanja in obveščanja.

Sodišče je nazadnje dodalo, da kadar upravljavec iskalnika ne ugodi zahtevi za odstranitev povezav, mora imeti oseba, na katero se nanašajo osebni podatki, možnost, da se obrne na nadzorni ali sodni organ, da ta opravi potrebna preverjanja in temu upravljavcu odredi sprejetje ukrepov, ki so potrebni. V zvezi s tem morajo zlasti sodni organi zagotoviti tehtanje nasprotujočih si interesov, saj so ti v najboljšem položaju za izvedbo kompleksnega in poglobljenega tehtanja, pri katerem se upoštevajo vsa merila in vsi elementi, določeni z upoštevno sodno prakso.

Na drugem mestu, Sodišče je razsodilo, je treba v okviru tehtanja zgoraj navedenih temeljnih pravic za namene obravnave zahteve za odstranitev povezav, katere cilj je, da se s seznama zadetkov slikovnega iskanja na podlagi imena fizične osebe odstranijo fotografije, prikazane v obliki predoglednih sličic, ki upodabljajo to osebo, upoštevati informativno vrednost teh fotografij, neodvisno od prvotnega konteksta njihove objave na spletni strani, s katere so povzete. Vendar je treba upoštevati vsak tekstualen element, ki neposredno spremlja prikaz teh fotografij med zadetki iskanja in ki lahko pojasni njihovo informativno vrednost.

Sodišče je zato, da je prišlo do tega sklepa, poudarilo, da za iskanja slik, ki se opravijo prek spletnega iskalnika na podlagi imena osebe, veljajo enaka načela kot za iskanje spletnih strani in na njih vsebovanih informacij. Navedlo je, da prikaz, in sicer v obliki predoglednih sličic – po iskanju na podlagi imena – fotografij osebe, na katero se nanašajo osebni podatki, lahko pomeni posebej velik poseg v pravici do varstva zasebnega življenja in osebnih podatkov te osebe.

Zato mora upravljavec iskalnika, kadar prejme zahtevo za odstranitev povezav, katere cilj je, da se iz zadetkov slikovnega iskanja na podlagi imena osebe odstranijo fotografije, prikazane v obliki predoglednih sličic, ki upodabljajo to osebo, preveriti, ali je prikaz zadevnih fotografij nujen za uresničevanje pravice do svobode obveščanja spletnih uporabnikov, ki so potencialno zainteresirani za dostop do teh fotografij prek takega iskanja.

Ker pa iskalnik prikazuje fotografije zadevne osebe zunaj konteksta, v katerem so te objavljene na spletni strani, uvrščeni na seznam zadetkov, najpogosteje za ilustracijo tekstualnih elementov, ki jih vsebuje ta stran, je treba ugotoviti, ali je treba ta kontekst vseeno upoštevati pri tehtanju nasprotujočih si pravic in interesov, ki ga je treba opraviti. V tem okviru je vprašanje, ali mora navedena presoja vključevati tudi vsebino spletne strani, na kateri je fotografija, za katero se zahteva odstranitev prikazovanja v obliki predogledne sličice, odvisno od predmeta in narave zadevne obdelave.

Prvič, glede predmeta zadevne obdelave je Sodišče ugotovilo, da ima lahko objava fotografij kot neverbalno komunikacijsko sredstvo večji vpliv na spletne uporabnike kot

tekstovne publikacije. Fotografije so namreč kot take pomembno sredstvo za pritegnitev pozornosti spletnih uporabnikov in lahko sprožijo interes za dostop do člankov, ki jih ilustrirajo. Vendar ker se fotografije pogosto lahko razlagajo na več načinov, lahko njihova objava – kot predogledne sličice – na seznamu zadetkov iskanja povzroči posebej grob poseg v pravico zadevne osebe do varstva njene podobe, kar je treba upoštevati pri tehtanju nasprotujočih si pravic in interesov. Potrebno je ločeno tehtanje glede na to, ali gre na eni strani za članke s fotografijami, ki jih objavi izdajatelj spletne strani in ki – vstavljene v svoj prvotni kontekst – ilustrirajo informacije iz tega članka in mnenja, ki so v njem izražena, ter na drugi strani za fotografije, ki jih v obliki predoglednih sličic na seznamu zadetkov prikaže upravljavec iskalnika zunaj konteksta, v katerem so bile objavljene na izvorni spletni strani.

V zvezi s tem je Sodišče opozorilo, da razlog, ki upravičuje objavo osebnega podatka na spletnem mestu, ni nujno enak razlogu, ki se uporabi za dejavnost iskalnikov, in da je, kadar je razlog enak, rezultat tehtanja zadevnih pravic in interesov, ki ga je treba opraviti, lahko različen glede na to, ali gre za obdelavo, ki jo izvede upravljavec iskalnika, ali obdelavo, ki jo izvede izdajatelj te spletne strani. Po eni strani so lahko legitimni interesi, ki upravičujejo obdelavo, različni, po drugi strani pa posledice teh obdelav za osebo, na katero se nanašajo osebni podatki, in zlasti za njeno zasebno življenje niso nujno enake.

Drugič, glede narave obdelave, ki jo izvede upravljavec iskalnika, je Sodišče ugotovilo, da upravljavec iskalnika s tem, da povzame fotografije fizičnih oseb, ki so objavljene na spletu, in jih ločeno prikaže v zadetkih slikovnega iskanja v obliki predoglednih sličic, ponudi storitev, ki zajema obdelavo osebnih podatkov, ki je avtonomna in ločena od obdelave izdajatelja spletne strani, s katere so fotografije povzete, ter obdelave, za katero je ta upravljavec ravno tako odgovoren, glede uvrstitve te strani na seznam zadetkov.

Zato je potrebna avtonomna presoja dejavnosti upravljavca iskalnika, ki obsega prikazovanje zadetkov slikovnega iskanja v obliki predoglednih sličic, saj je lahko dodaten poseg v temeljne pravice, ki je posledica take dejavnosti, posebej intenziven, ker se pri iskanju po imenu združujejo vse informacije, ki se nanašajo na zadevnega posameznika, ki so na spletu. V okviru te avtonomne presoje je treba upoštevati dejstvo, da je ta prikaz sam po sebi zadetek, ki ga išče spletni uporabnik, ne glede na njegovo poznejšo odločitev, ali bo dostopil do prvotne spletne strani.

Vendar je Sodišče ugotovilo, da tako posebno tehtanje, pri katerem se upošteva avtonomnost obdelave, ki jo izvaja upravljavec iskalnika, ne vpliva na morebitno upoštevnost tekstualnih elementov, ki lahko neposredno spremljajo prikaz fotografije na seznamu zadetkov iskanja, saj se lahko s takimi elementi pojasni informativna vrednost te fotografije za javnost ter ti elementi tako lahko vplivajo na tehtanje zadevnih pravic in interesov.

4. Privolitev uporabnika spletnega mesta v shranjevanje informacij

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

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[94] v povezavi z Direktivo 95/46[95] ter SUVP[96].

Prvič, Sodišče je navedlo, da člen 2(h) Direktive 95/46/ES, 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 SUVP[97], 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.

---

94 Člena 2(f) in 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).

95 Člen 2(h) Direktive 95/46.

96 Člen 6(1)(a) Uredbe 2016/679.

97 Prav tam.

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 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.

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.

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.

5. Obdelava osebnih podatkov na spletnih družbenih omrežjih

Sodba z dne 4. julija 2023 (veliki senat), Meta Platforms in drugi (Splošni pogoji za uporabo družbenega omrežja) (C-252/21,* EU:C:2023:537*)

Družba Meta Platforms je lastnica spletnega družbenega omrežja „Facebook“, ki je za zasebne uporabnike brezplačno. Poslovni model tega družbenega omrežja temelji na financiranju prek spletnega oglaševanja, ki se izvaja po meri za njegove posamezne uporabnike. Tako oglaševanje je tehnično izvedljivo z avtomatizirano določitvijo podrobnih profilov uporabnikov omrežja in spletnih storitev, ki se ponujajo na ravni skupine Meta. Tako morajo uporabniki, da bi lahko uporabljali navedeno družbeno omrežje, ob svojem vpisu sprejeti splošne pogoje, ki jih je določila družba Meta Platforms ter ki napotujejo na politike uporabe podatkov in piškotkov, ki jih je določila ta družba. Na podlagi teh politik družba Meta Platforms poleg podatkov, ki jih ti uporabniki vnesejo neposredno ob svojem vpisu, zbira tudi podatke v zvezi z dejavnostmi navedenih uporabnikov znotraj in zunaj družbenega omrežja, ter te podatke poveže z računi zadevnih uporabnikov na Facebooku. Glede zadnjenavedenih podatkov, ki se imenujejo tudi „podatki *off* Facebook“, gre na eni strani za podatke v zvezi z obiskom tretjih spletnih strani in aplikacij in na drugi strani za podatke v zvezi z uporabo drugih spletnih storitev, ki spadajo v skupino Meta (med katerimi sta Instagram in WhatsApp).

Na podlagi splošnega pregleda tako zbranih podatkov je mogoče izpeljati podrobne ugotovitve o preferencah in interesih teh uporabnikov.

Bundeskartellamt (zvezni urad za varstvo konkurence, Nemčija) je z odločbo z dne 6. februarja 2019 družbi Meta Platforms prepovedal, prvič, da v tedaj veljavnih splošnih pogojih uporabo družbenega omrežja Facebook s strani zasebnih uporabnikov, ki prebivajo v Nemčiji, pogojuje z obdelavo njihovih podatkov *off* Facebook in, drugič, da te podatke obdeluje brez njihove privolitve. Poleg tega ji je zvezni urad za varstvo konkurence naložil, naj te splošne pogoje prilagodi, tako da bi bilo iz njih jasno razvidno, da navedeni podatki ne bodo zbrani, povezani z računi uporabnikov na Facebooku in uporabljeni brez privolitve zadevnih uporabnikov. Nazadnje, ta organ je poudaril, da taka privolitev ni veljavna, če je ta pogoj za uporabo družbenega omrežja. Svojo odločbo je utemeljil z dejstvom, da zadevna obdelava podatkov, ki naj ne bi bila v skladu s SUVP, pomeni zlorabo prevladujočega položaja družbe Meta Platforms na trgu spletnih družbenih omrežij.

Družba Meta Platforms je zoper to odločbo vložila tožbo pri Oberlandesgericht Düsseldorf (višje deželno sodišče v Düsseldorfu, Nemčija). Ker je višje deželno sodišče v Düsseldorfu dvomilo med drugim o razlagi nekaterih določb SUVP, je pri Sodišču vložilo predlog za sprejetje predhodne odločbe.

Sodišče, ki je zasedalo v velikem senatu, je podalo pojasnila glede tega, ali lahko operater družbenega omrežja obdeluje „občutljive“ osebne podatke svojih uporabnikov, glede pogojev za zakonitost obdelave podatkov, ki jo izvaja tak operater, ter glede veljavnosti privolitve, ki jo ti uporabniki za tako obdelavo dajo podjetju s prevladujočim položajem na nacionalnem trgu spletnih družbenih omrežij.

Sodišče je v zvezi z obdelavo posebnih vrst osebnih podatkov[98] ocenilo, da če uporabnik spletnega družbenega omrežja obišče spletna mesta ali aplikacije v povezavi z eno ali več temi kategorijami in po potrebi na teh spletnih mestih ali v te aplikacije vnese podatke tako, da se vpiše ali opravlja spletna naročila, je treba obdelavo osebnih podatkov, ki jo opravlja operater tega spletnega družbenega omrežja,[99] šteti za „obdelavo posebnih vrst osebnih podatkov“ v smislu člena 9(1) SUVP, če ta obdelava omogoča razkritje informacij, ki spadajo v eno od teh kategorij, ne glede na to, ali se te informacije nanašajo na uporabnika tega omrežja ali na katerega koli drugega posameznika. Taka obdelava podatkov je, s pridržkom nekaterih odstopanj[100], načeloma prepovedana.

---

98 Iz člena 9(1) SUVP. V tej določbi je predpisano, da „[sta] prepovedani […] obdelava osebnih podatkov, ki razkrivajo rasno ali etnično poreklo, politično mnenje, versko ali filozofsko prepričanje ali članstvo v sindikatu, in obdelava genetskih podatkov, biometričnih podatkov za namene edinstvene identifikacije posameznika, podatkov v zvezi z zdravjem ali podatkov v zvezi s posameznikovim spolnim življenjem ali spolno usmerjenostjo“.

99 Ta obdelava zajema zbiranje – prek integriranih vmesnikov, piškotkov ali podobnih tehnologij za zapisovanje – podatkov, ki izhajajo iz obiska teh spletnih mest in teh aplikacij, ter podatkov, ki jih je vnesel uporabnik, povezovanje vseh teh podatkov z računom tega uporabnika na družbenem omrežju in uporabo teh podatkov s strani tega operaterja.

100 Določenih v členu 9(2) SUVP. V tej določbi je navedeno: „Odstavek 1 se ne uporablja, če velja eno od naslednjega:

V zvezi z zadnjenavedenim je Sodišče pojasnilo, da kadar uporabnik spletnega družbenega omrežja obišče spletna mesta ali aplikacije v povezavi z eno ali več navedenih posebnih kategorij podatkov, podatkov v zvezi s tem obiskom, ki jih upravljavec tega spletnega družbenega omrežja zbere prek piškotkov ali podobnih tehnologij za zapisovanje, ne objavi sam.[101] Poleg tega, kadar uporabnik vnese podatke na taka spletna mesta ali v take aplikacije ali klikne na izbirna polja, ki so integrirana v ta spletna mesta ali v te aplikacije, kot so polja „všeč mi je“ ali „deli z drugimi“ oziroma polja, ki uporabniku omogočajo, da se na teh spletnih mestih ali v teh aplikacijah identificira z uporabo identifikatorjev povezave, povezanih z njegovim uporabniškim računom na družbenem omrežju, z njegovo telefonsko številko ali z njegovim elektronskim naslovom, tak uporabnik tako vstavljene podatke ali podatke, ki izhajajo iz klika na ta polja, objavi sam le v primeru, da je predhodno izrecno izrazil svojo izbiro – po potrebi na podlagi individualnih nastavitev, uporabljenih ob polnem poznavanju zadeve – da so podatki, ki se nanašajo nanj, javno dostopni neomejenemu številu oseb.

Sodišče je glede, splošneje, pogojev za zakonitost obdelave osebnih podatkov opozorilo, da je na podlagi SUVP obdelava podatkov zakonita, če in kolikor je posameznik, na katerega se nanašajo osebni podatki, v to obdelavo privolil v enega ali več določenih namenov.[102] Če take privolitve ni ali če ta privolitev ni bila dana prostovoljno, izrecno, informirano in nedvoumno, je taka obdelava vseeno upravičena, če izpolnjuje eno od zahtev nujnosti[103], ki jih je treba razlagati ozko. Obdelava osebnih podatkov uporabnikov, ki jo izvaja operater spletnega družbenega omrežja, se lahko šteje za potrebno za izvajanje pogodbe, katere pogodbene stranke so ti uporabniki, le, če je ta obdelava objektivno nujna za uresničitev cilja, ki je sestavni del pogodbene dajatve, namenjene tem uporabnikom, tako da če te obdelave ni, glavnega predmeta pogodbe ni mogoče uresničiti.

Poleg tega je Sodišče navedlo, da se zadevna obdelava podatkov lahko šteje za potrebno zaradi zakonitih interesov, za katere si prizadeva upravljavec ali tretja oseba, le, če je navedeni operater uporabnikom, od katerih so bili podatki zbrani, navedel zakoniti interes, ki mu sledi obdelava teh podatkov, če se ta obdelava izvaja v mejah nujno potrebnega za uresničitev tega zakonitega interesa in če iz tehtanja nasprotujočih si interesov glede na vse upoštevne okoliščine izhaja, da interesi ali temeljne svoboščine in pravice teh uporabnikov ne prevladajo nad navedenim zakonitim interesom upravljavca ali tretje osebe. Sodišče pa je med drugim ocenilo, da interesi in temeljne pravice

(a) posameznik, na katerega se nanašajo osebni podatki, je dal izrecno privolitev v obdelavo navedenih osebnih podatkov za enega ali več določenih namenov, razen kadar pravo Unije ali pravo države članice določa, da posameznik, na katerega se nanašajo osebni podatki, ne sme odstopiti od prepovedi iz odstavka 1; […]

(e) obdelava je povezana z osebnimi podatki, ki jih posameznik, na katerega se nanašajo osebni podatki, sam objavi;

(f) obdelava je potrebna za uveljavljanje, izvajanje ali obrambo pravnih zahtevkov ali kadar koli sodišča izvajajo svojo sodno pristojnost;

[…]“

101 V smislu člena 9(2)(e) SUVP.

102 V skladu s členom 6(1), prvi pododstavek, točka (a), SUVP.

103 Omenjenih v členu 6(1), prvi pododstavek, točke od (b) do (f), SUVP. V skladu s temi določbami je obdelava zakonita, le če in kolikor je med drugim potrebna za izvajanje pogodbe, katere pogodbena stranka je posameznik, na katerega se nanašajo osebni podatki (člen 6(1), prvi pododstavek, točka (b), SUVP), za izpolnitev zakonske obveznosti, ki velja za upravljavca (člen 6(1), prvi pododstavek, točka (c), SUVP), ali zaradi zakonitih interesov, za katere si prizadeva upravljavec ali tretja oseba (člen 6(1), prvi pododstavek, točka (f), SUVP).

navedenih uporabnikov ob neobstoju njihove privolitve prevladajo nad interesom upravljavca spletnega družbenega omrežja za personalizacijo oglaševanja, s katerim financira svojo dejavnost.

Nazadnje, Sodišče je pojasnilo, da je zadevna obdelava podatkov upravičena, kadar je dejansko potrebna za izpolnitev zakonske obveznosti, ki velja za upravljavca, na podlagi določbe prava Unije ali prava zadevne države članice, če ta pravna podlaga izpolnjuje cilj javnega interesa in je sorazmerna z zakonitim ciljem, za katerega si prizadeva, in če se ta obdelava izvede v mejah tistega, kar je nujno potrebno.

V zvezi z veljavnostjo privolitve zadevnih uporabnikov v obdelavo njihovih podatkov na podlagi SUVP je Sodišče ocenilo, da okoliščina, da ima operater spletnega družbenega omrežja prevladujoč položaj na trgu spletnih družbenih omrežij, sama po sebi ni ovira za to, da lahko uporabniki takega omrežja podajo veljavno privolitev v obdelavo svojih osebnih podatkov, ki jo izvede ta operater. Vendar tak položaj, glede na to, da lahko vpliva na svobodno izbiro teh uporabnikov in ustvari očitno neravnotežje med njimi in navedenim operaterjem, pomeni pomemben element pri ugotavljanju, ali je bila privolitev dejansko podana veljavno in zlasti prostovoljno, kar mora dokazati navedeni operater.[104]

Natančneje, uporabniki zadevnega družbenega omrežja morajo imeti svobodo, da v okviru pogodbenega procesa posamično zavrnejo privolitev za specifična dejanja obdelave podatkov, ki niso potrebna za izvajanje pogodbe, ne da bi se morali v celoti odpovedati uporabi tega spletnega družbenega omrežja, kar pomeni, da se navedenim uporabnikom po potrebi za ustrezno plačilo ponudi enakovredna alternativa, ki ni povezana s takimi dejanji obdelave podatkov. Poleg tega mora obstajati možnost, da se za obdelavo podatkov *off* Facebook poda ločena privolitev.

[104] Na podlagi člena 7(1) SUVP.

VI. Nacionalni nadzorni organi

1. Obseg zahteve po neodvisnosti

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

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 zadnjenavedeni 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 nanašajo, zaradi česar morajo nadzorni organi pri izvajanju nalog ravnati objektivno in nepristransko.

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.

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.

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.

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 določen 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.

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

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/ES ne izpolni država članica, ki predčasno prekine mandat nadzornega organa za varstvo osebnih podatkov.

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.

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 vsakršnih okoliščinah deluje brez vsakega suma pristranskosti.

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

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

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

Kúria (vrhovno sodišče, Madžarska), ki mu je bila predložena kasacijska pritožba, je dvomilo o določitvi prava, ki se uporablja, 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 uporablja, 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 mest 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, na katere se nanaša ta obdelava podatkov.

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. Vendar če ugotovi, da se uporablja 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.

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.

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.

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, da preveri, ali prenos osebnih podatkov iz države članice, ki ji pripada, v tretjo državo izpolnjuje zahteve, določene v tej direktivi.

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

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.

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[105] 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 SUVP[106], na pristojnosti APD in se je, natančneje, spraševalo, ali lahko APD za dejstva, ki so nastala po začetku veljavnosti SUVP, 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 SUVP naj bi bil namreč za vložitev opustitvene tožbe pristojen le irski pooblaščenec za varstvo podatkov, pod nadzorom irskih sodišč.

Sodišče je s sodbo, izdano v velikem senatu, pojasnilo, katera so pooblastila nacionalnih nadzornih organov v okviru SUVP. 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 SUVP in začne sodni postopek v zvezi s čezmejno obdelavo podatkov,[107] čeprav ni vodilni nadzorni organ glede take obdelave.

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 SUVP in po potrebi začne sodni postopek, da bi bila zagotovljena uporaba te uredbe. Tako mora biti s SUVP temu nadzornemu organu po eni strani podeljena pristojnost za sprejemanje odločb o ugotovitvi, da so z navedeno obdelavo kršena pravila, ki jih ta

105 Na primer gumba „všeč mi je“ ali „deli“.

106 Člen 56(1) SUVP 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.“

107 V smislu člena 4, točka 23, SUVP.

uredba vsebuje, po drugi strani pa je treba to pooblastilo izvajati ob spoštovanju postopka sodelovanja in postopka za skladnost iz te uredbe.[108]

SUVP namreč za čezmejne obdelave določa mehanizem „vse na enem mestu“,[109] 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 SUVP 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,[110] medtem ko je pristojnost drugih nacionalnih nadzornih organov za sprejetje take odločbe, tudi začasne, izjema.[111] 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.

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 te države članice opozori na vsakršno domnevno kršitev SUVP in po potrebi začne sodni postopek, izvršuje le ob upoštevanju pravil o razdelitvi pristojnosti odločanja med vodilnim nadzornim organom in drugimi nadzornimi organi,[112] 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.

Sodišče je na drugem mestu razsodilo, da izvrševanje pooblastila nadzornega organa države članice, ki ni vodilni nadzorni organ, da začne sodni postopek,[113] 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 SUVP,[114] kar pomeni, da mora imeti upravljavec ali obdelovalec čezmejne obdelave poslovno enoto na ozemlju Unije.

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 SUVP in po potrebi začne sodni postopek, v primeru čezmejne obdelave podatkov mogoče izvrševati tako glede glavne poslovne enote upravljavca, ki je

108 Določenih v členih 56 in 60 SUVP.
109 Člen 56(1) SUVP.
110 Člen 60(7) SUVP.
111 Člen 56(2) in člen 66 SUVP določata izjeme od načela pristojnosti vodilnega nadzornega organa za odločanje.
112 Določena v členih 55 in 56 v povezavi s členom 60 SUVP.
113 V skladu s členom 58(5) SUVP.
114 Člen 3(1) SUVP 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“.

v državi 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 SUVP 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 SUVP.

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 SUVP, 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 SUVP, 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.

Sodišče je na petem in zadnjem mestu priznalo neposredni učinek določbe SUVP, 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.

Sodba z dne 16. januarja 2024 (veliki senat), Österreichische Datenschutzbehörde (C-33/22, EU:C:2024:46)

Sodišče je v tej zadevi (glej tudi razdelek II.1., naslovljen „Področje uporabe splošne ureditve“) navedlo, da določbe SUVP v zvezi s pristojnostjo nacionalnih nadzornih organov in pravico do pritožbe[115] ne zahtevajo sprejetja nacionalnih izvedbenih ukrepov ter so dovolj jasne, natančne in brezpogojne, da imajo neposreden učinek. Iz tega sledi, da čeprav je s SUVP državam članicam priznano polje proste presoje glede števila nadzornih organov, ki jih je treba ustanoviti,[116] je z njo določen obseg pristojnosti teh organov za nadzor nad uporabo SUVP. Tako ima v primeru, če se država članica odloči ustanoviti en sam nacionalni nadzorni organ, ta nujno vse pristojnosti, določene s to

[115] Člen 55(1) in člen 77(1) SUVP.
[116] V skladu s členom 51(1) SUVP.

uredbo. Vsaka drugačna razlaga bi ogrozila polni učinek teh določb in bi lahko oslabila polni učinek vseh drugih določb SUVP, na katere bi se lahko nanašala pritožba.

V zvezi z okoliščino, da nacionalne določbe na ustavni ravni izključujejo možnost nadzornega organa, ki je odvisen od izvršilne oblasti, da nadzira uporabo SUVP s strani organa, ki spada pod zakonodajno oblast, je Sodišče poudarilo, da SUVP prav zaradi spoštovanja ustavne strukture držav članic zahteva le, da države članice ustanovijo vsaj en nadzorni organ, hkrati pa jim daje možnost, da jih ustanovijo več. Ta uredba tako vsaki državi članici priznava polje proste presoje, ki ji omogoča, da ustanovi toliko nadzornih organov, kolikor jih je potrebnih med drugim na podlagi zahtev v zvezi z njeno ustavno ureditvijo.

Poleg tega to, da se država članica sklicuje na določbe nacionalnega prava, ne sme posegati v enotnost in učinkovitost prava Unije. Učinki načela primarnosti prava Unije so namreč zavezujoči za vse organe države članice, ne da bi med drugim nacionalne določbe, vključno s tistimi na ustavni ravni, to lahko ovirale.

Če se je torej država članica odločila ustanoviti en sam nadzorni organ, se ne more sklicevati na določbe nacionalnega prava, vključno s tistimi na ustavni ravni, da bi obdelave osebnih podatkov, ki spadajo na področje uporabe SUVP, izvzela iz nadzora tega organa.

4. Pogoji za naložitev upravnih glob

Sodba z dne 5. decembra 2023 (veliki senat), Nacionalinis visuomenės sveikatos centras (C-683/21, EU:C:2023:949)

Sodišče je v tej zadevi (glej tudi razdelke II.3., II.5. in II.6., naslovljene „Pojem ‚obdelava osebnih podatkov‘“, „Pojem ‚upravljavec osebnih podatkov‘“ in „Pojem ‚skupni upravljavec‘“) ugotovilo, da se lahko na podlagi člena 83 SUVP upravna globa upravljavcu naloži le, če se ugotovi, da je namerno ali iz malomarnosti kršil pravila iz te uredbe[117].

V zvezi s tem je Sodišče pojasnilo, da zakonodajalec Unije državam članicam ni pustil polja proste presoje glede vsebinskih pogojev, ki jih mora nadzorni organ spoštovati, kadar se odloči upravljavcu naložiti upravno globo na podlagi te določbe. Dejstvo, da SUVP državam članicam daje možnost, da določijo izjeme glede javnih organov in teles, ustanovljenih na njihovem ozemlju,[118] ter zahteve v zvezi s postopkom, po katerem

[117] Kršitev iz člena 83, od (4) do (6), SUVP.

[118] Na podlagi člena 83(7) SUVP, ki določa, da „[...] lahko vsaka država članica določi pravila o tem, ali in v kolikšni meri se lahko javnim organom in telesom z ustanovitvijo v zadevni državi članici naložijo upravne globe“.

morajo nadzorni organi naložiti upravno globo,[119] nikakor ne pomeni, da so te države pooblaščene tudi, da določijo take vsebinske pogoje.

Sodišče je v zvezi s temi pogoji navedlo, da je med elementi, naštetimi v SUVP, na podlagi katerih nadzorni organ upravljavcu naloži upravno globo, vključeno, da se ustrezno upošteva, „ali je kršitev naklepna ali posledica malomarnosti“[120]. Nobeden od teh elementov pa se ne nanaša na kakršno koli možnost uveljavljanja odgovornosti upravljavca, če ni podana njegova krivda. Tako je mogoče le zaradi kršitev določb SUVP, ki jih upravljavec stori namerno ali iz malomarnosti, temu upravljavcu na podlagi člena 83 te uredbe naložiti upravno globo.

Sodišče je dodalo, da to razlago potrjujeta splošna sistematika in namen SUVP. V tem okviru je Sodišče pojasnilo, da obstoj sistema sankcij na podlagi SUVP, ki omogoča, da se upravljavcem in obdelovalcem, če to upravičujejo posebne okoliščine vsakega posameznega primera, naloži upravna globa, spodbuja upravljavce in obdelovalce, da ravnajo v skladu s to uredbo, in da upravne globe z odvračilnim učinkom prispevajo h krepitvi varstva posameznikov, na katere se nanašajo osebni podatki. Vendar je zakonodajalec Unije menil, da ni treba določiti naložitve upravnih glob v primeru, da krivda ni podana. Glede na to, da je namen Splošne pogodbe o varstvu podatkov hkrati enakovredna in enotna raven varstva in da jo je treba zato dosledno uporabljati v celotni Uniji, bi bilo v nasprotju s tem ciljem, če bi se državam članicam dovolilo, da določijo tako ureditev za naložitev globe.

Poleg tega je Sodišče ugotovilo, da se taka globa lahko naloži upravljavcu v zvezi z dejanji obdelave osebnih podatkov, ki jih izvede obdelovalec v imenu tega upravljavca, razen če ta obdelovalec v okviru teh dejanj izvede obdelavo zaradi svojih ciljev ali če je te podatke obdelal na način, ki ni združljiv z okvirom ali pravili obdelave, kot jih je določil upravljavec, ali tako, da ni mogoče razumno šteti, da je upravljavec v to privolil. V takem primeru je treba obdelovalca šteti za upravljavca take obdelave.

Sodba z dne 5. decembra 2023 (veliki senat), Deutsche Wohnen (C-807/21, EU:C:2023:950)

Deutsche Wohnen SE (v nadaljevanju: DW) je nepremičninska družba, ki ima posredno, prek deležev v različnih družbah, v lasti številne poslovne in stanovanjske enote. V okviru svojih poslovnih dejavnosti obdeluje osebne podatke najemnikov teh enot.

Berliner Beauftragte für den Datenschutz (organ za varstvo podatkov v Berlinu, Nemčija, v nadaljevanju: nadzorni organ) je po dveh pregledih, opravljenih v letih 2017 in 2019, ugotovil vrsto kršitev SUVP, ki jih je storila družba DW. Ta nadzorni organ je tej družbi z odločbo z dne 30. oktobra 2019 na tej podlagi naložil upravne globe.

[119] Na podlagi člena 83(8) SUVP v povezavi z uvodno izjavo 129 te uredbe.
[120] Člen 83(2)(b) SUVP.

Družba DW je zoper to odločbo vložila tožbo pri Landgericht Berlin (deželno sodišče v Berlinu, Nemčija), ki je postopek ustavilo. To sodišče je poudarilo, da je v skladu z nemškim pravom[121] upravni prekršek mogoče ugotoviti le za fizično osebo, ne pa za pravno osebo. Poleg tega naj bi bilo mogoče pravni osebi v primeru vzpostavitve njene odgovornosti pripisati le dejanja članov njenih organov ali njenih zastopnikov. Staatsanwaltschaft Berlin (državno tožilstvo v Berlinu, Nemčija) je to odločbo izpodbijalo pred Kammergericht Berlin (višje deželno sodišče v Berlinu, Nemčija). V teh okoliščinah je to sodišče pri Sodišču vložilo predlog za sprejetje predhodne odločbe glede razlage SUVP.

Sodišče, ki je zasedalo v velikem senatu, je v sodbi odločilo o pogojih za naložitev upravnih glob na podlagi SUVP. Na prvem mestu, preučilo je vprašanje, ali lahko države članice naložitev upravne globe pravni osebi pogojujejo s tem, da je bila kršitev te uredbe predhodno pripisana določeni fizični osebi. Na drugem mestu, podobno kot v zadevi Nacionalinis visuomenės sveikatos centras (glej zgoraj), je obravnavalo vprašanje, ali je treba sankcionirano kršitev določb SUVP storiti namerno ali iz malomarnosti.

V zvezi z naložitvijo upravne globe na podlagi SUVP pravni osebi je Sodišče najprej navedlo, da se načela, prepovedi in obveznosti iz SUVP nanašajo zlasti na „upravljavce“, katerih odgovornost se razteza na vsako obdelavo osebnih podatkov, ki jo izvedejo upravljavci ali je izvedena v njihovem imenu. V primeru kršitve določb SUVP je ta odgovornost podlaga za naložitev upravne globe upravljavcu na podlagi člena 83 te uredbe. Vendar zakonodajalec Unije za namene ugotavljanja take odgovornosti ni razlikoval med fizičnimi in pravnimi osebami, saj je ta odgovornost pogojena le s tem, da te osebe same ali skupaj z drugimi določijo namene in sredstva obdelave osebnih podatkov.[122] Zato je vsaka oseba, ki izpolnjuje ta pogoj, odgovorna zlasti za vsako kršitev SUVP, ki jo stori sama ali je storjena v njenem imenu. To na eni strani pomeni, da pravne osebe niso odgovorne le za kršitve, ki jih storijo njihovi zastopniki, direktorji ali poslovodje, ampak tudi za kršitve katere koli druge osebe, ki deluje v okviru gospodarske dejavnosti teh pravnih oseb in v njihovem imenu. Na drugi strani mora obstajati možnost, da se upravne globe, ki so v SUVP določene za take kršitve, naložijo neposredno pravnim osebam, kadar je te osebe mogoče opredeliti kot upravljavce.

Dalje, Sodišče je opozorilo, da na podlagi nobene določbe SUVP ni mogoče šteti, da bi bila naložitev upravne globe pravni osebi kot upravljavcu pogojena s predhodno ugotovitvijo, da je to kršitev storila določena fizična oseba. Poleg tega zakonodajalec Unije državam članicam v zvezi s tem ni pustil polja proste presoje. Vendar dejstvo, da SUVP državam članicam daje možnost, da določijo zahteve glede postopka, ki ga morajo nadzorni organi izvesti za naložitev upravne globe,[123] nikakor ne pomeni, da bi bile te

[121] Gesetz über Ordnungswidrigkeiten (zakon o prekrških) z dne 24. maja 1968 (BGBl. 1968 I, str. 481) v različici iz obvestila z dne 19. februarja 1987 (BGBl. 1987 I str. 602), kakor je bil spremenjen z zakonom z dne 19. junija 2020 (BGBl. 2020 I, str. 1350).

[122] V skladu s členom 4, točka 7, SUVP.

[123] Kot izhaja iz člena 58(4) in člena 83(8) SUVP v povezavi z uvodno izjavo 129 te uredbe.

države članice pooblaščene tudi za določitev dodatnih vsebinskih pogojev poleg tistih iz SUVP.

V tem okviru je Sodišče pojasnilo, da če bi se državam članicam dovolilo, da enostransko in kot nujni pogoj za naložitev upravne globe na podlagi člena 83 SUVP upravljavcu, ki je pravna oseba, zahtevajo, da se zadevna kršitev predhodno pripiše ali lahko pripiše določeni fizični osebi, bi bilo to v nasprotju z namenom SUVP. Poleg tega bi taka dodatna zahteva nazadnje lahko oslabila učinkovitost in odvračilni učinek upravnih glob, naloženih pravnim osebam kot upravljavcem.

Nazadnje, Sodišče je poudarilo, da pojem „podjetje“ v smislu členov 101 in 102 PDEU[124] ne vpliva na vprašanje, ali in pod katerimi pogoji je mogoče upravljavcu, ki je pravna oseba, na podlagi člena 83 SUVP naložiti upravno globo, in je upošteven le za določitev zneska take globe.

Sodišče je tako ugotovilo, da SUVP[125] nasprotuje nacionalni ureditvi, v skladu s katero je mogoče pravni osebi kot upravljavcu upravno globo za kršitev te uredbe[126] naložiti le, če je bila ta kršitev predhodno pripisana določeni fizični osebi.

V zvezi z vprašanjem, ali lahko države članice določijo naložitev upravne globe, tudi če sankcionirana kršitev ni bila storjena namerno ali iz malomarnosti, je Sodišče najprej opozorilo, da vsebinski pogoji, ki jih mora nadzorni organ spoštovati, kadar upravljavcu naloži tako globo, spadajo izključno na področje uporabe prava Unije in da države članice v zvezi s tem nimajo nobenega manevrskega prostora. Sodišče na podlagi enakega razlogovanja kot v zgoraj navedeni sodbi Nacionalinis visuomenės sveikatos centras précité ugotovilo, da je mogoče v skladu s členom 83 SUVP upravno globo naložiti le, če je dokazano, da je upravljavec, ki je hkrati pravna oseba in podjetje, namerno ali iz malomarnosti kršil pravila iz te uredbe.

5. Povezava pristojnosti nacionalnih nadzornih organov s pristojnostmi drugih nacionalnih organov

Sodba z dne 4. julija 2023 (veliki senat), Meta Platforms in drugi (Splošni pogoji za uporabo družbenega omrežja) (C-252/21, EU:C:2023:537)

V tej zadevi (glej tudi razdelek V.5., naslovljen „Obdelava osebnih podatkov na spletnih družbenih omrežjih“) je Sodišče v okviru odločanja v zvezi s pristojnostjo organa, pristojnega za konkurenco, za ugotavljanje neskladnosti obdelave osebnih podatkov s SUVP ugotovilo, da lahko tak organ, s pridržkom spoštovanja svoje obveznosti lojalnega

124 Na katerega je napoteno v uvodni izjavi 150 SUVP.
125 Člen 58(2)(i) in člen 83, od (1) do (6), SUVP.
126 Iz člena 83, od (4) do (6), SUVP.

sodelovanja[127] z nadzornimi organi za varstvo podatkov, v okviru preizkusa zlorabe prevladujočega položaja s strani podjetja ugotovi,[128] da splošni pogoji uporabe tega podjetja v zvezi z obdelavo osebnih podatkov in njihovo izvajanje niso v skladu s to uredbo, če je ta ugotovitev potrebna za ugotovitev obstoja take zlorabe. Vendar kadar organ, pristojen za konkurenco, v okviru ugotovitve zlorabe prevladujočega položaja ugotovi kršitev SUVP, ne nadomesti nadzornih organov.

Tako se morajo organi, pristojni za konkurenco, ob upoštevanju načela lojalnega sodelovanja, kadar morajo pri izvajanju svojih pristojnosti preizkusiti skladnost ravnanja podjetja z določbami SUVP, posvetovati in lojalno sodelovati z zadevnimi nacionalnimi nadzornimi organi ali vodilnim nadzornim organom. Vsi ti organi morajo torej spoštovati svoja pooblastila in pristojnosti, tako da se spoštujejo obveznosti, ki izhajajo iz SUVP, in cilji te uredbe ter da se ohrani njihov polni učinek. Iz tega sledi, da mora organ, pristojen za konkurenco, kadar v okviru preizkusa, katerega namen je ugotoviti, ali je podjetje zlorabilo prevladujoči položaj, meni, da je treba preučiti skladnost ravnanja tega podjetja z vidika določb SUVP, preveriti, ali je bilo to ravnanje ali podobno ravnanje že predmet odločitve pristojnega nacionalnega nadzornega organa ali vodilnega nadzornega organa ali celo Sodišča. Če je tako, organ, pristojen za konkurenco, od teh odločitev ne more odstopati, vendar lahko iz njih izpelje lastne sklepe z vidika uporabe konkurenčnega prava.

Kadar organ, pristojen za konkurenco, dvomi o obsegu presoje, ki jo opravi pristojni nacionalni nadzorni organ ali vodilni nadzorni organ, kadar ta organa istočasno preučujeta zadevno ravnanje ali podobno ravnanje, ali kadar ob neobstoju preiskave navedenih organov meni, da ravnanje podjetja ni v skladu z določbami SUVP, se mora navedeni organ posvetovati s tema organoma in ju prositi za sodelovanje, da se odpravijo njegovi dvomi ali ugotovi, ali je treba počakati, da zadevni nadzorni organ sprejme odločitev, preden začne lastno presojo. Če ta organa ne ugovarjata ali v razumnem roku ne odgovorita, lahko organ, pristojen za konkurenco, svojo preiskavo nadaljuje.

[127] Določene v členu 4(3) PEU.
[128] V smislu člena 102 PDEU.

SODIŠČE
EVROPSKE UNIJE

Direktorat za raziskave in dokumentacijo

Julij 2024