SUD
EUROPSKE UNIJE

HR

Tematski prikaz
Zaštita osobnih podataka

Uprava za istraživanje i dokumentaciju

curia.europa.eu

Predgovor

Pravo na zaštitu osobnih podataka temeljno je pravo čije poštovanje predstavlja važan cilj Europske unije.

Ono je utvrđeno primarnim pravom, osobito člankom 8. Povelje Europske unije o temeljnim pravima (u daljnjem tekstu: Povelja) i člankom 16. stavkom 1. Ugovora o funkcioniranju Europske unije (UFEU). To temeljno pravo također je usko povezano s pravom na poštovanje privatnog i obiteljskog života, koje je sadržano u članku 7. Povelje.

Kad je riječ o sekundarnom pravu, Europska zajednica od sredine 90-ih godina počela je donositi različite instrumente namijenjene jamčenju zaštite osobnih podataka. Direktiva 95/46/EZ o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom protoku takvih podataka[1], stavljena izvan snage 2018., predstavljala je u tom pogledu glavni pravni akt Unije u tom području.

Direktiva 95/46 dopunjena je zatim Direktivom 2002/58/EZ[2], kojom su se usklađivale odredbe zakonodavstava država članica o zaštiti prava na privatnost, osobito u pogledu obrade osobnih podataka u području elektroničkih komunikacija[3]. Valja istaknuti da je zakonodavac Unije, kako bi uzeo u obzir nova tehnološka i tržišna kretanja, od 2017. pokrenuo preispitivanje te direktive[4], koje je i danas u tijeku[5].

Europska unija reformirala je 2016. opći pravni okvir u tom području. U tu je svrhu donijela Uredbu (EU) 2016/679[6] o zaštiti osobnih podataka (u daljnjem tekstu: OUZP), kojom se stavlja izvan snage Direktiva 95/46 i koja se primjenjuje od 25. svibnja 2018.,

---

1 Direktiva 95/46/EZ Europskog parlamenta i Vijeća od 24. listopada 1995. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom protoku takvih podataka (SL 1995., L 281, str. 31.) (SL, posebno izdanje na hrvatskom jeziku, poglavlje 13., svezak 7., str. 88.), konsolidirana verzija od 20. studenoga 2003., stavljena izvan snage 25. svibnja 2018. (vidjeti bilješku 6.)

2 Direktiva 2002/58/EZ Europskog parlamenta i Vijeća od 12. srpnja 2002. o obradi osobnih podataka i zaštiti privatnosti u području elektroničkih komunikacija (Direktiva o privatnosti i elektroničkim komunikacijama) (SL 2002., L 201, str. 37.) (SL, posebno izdanje na hrvatskom jeziku, poglavlje 13., svezak 52., str. 111.), konsolidirana verzija od 19. prosinca 2009.

3 Direktiva 2002/58 izmijenjena je Direktivom 2006/24/EZ Europskog parlamenta i Vijeća od 15. ožujka 2006. o zadržavanju podataka dobivenih ili obrađenih u vezi s pružanjem javno dostupnih elektroničkih komunikacijskih usluga ili javnih komunikacijskih mreža i o izmjeni Direktive 2002/58/EZ (SL 2006., L 105, str. 54.) (SL, posebno izdanje na hrvatskom jeziku, poglavlje 13., svezak 50., str. 30.). Sud je presudom od 8. travnja 2014., Digital Rights Ireland i Seitlinger i dr. (C-293/12 i C-594/12, EU:C:2014:238) proglasio nevaljanom potonju direktivu jer je teško kršila prava na poštovanje privatnog života i zaštitu osobnih podataka (vidjeti poglavlje I.1. ovog prikaza, naslovljeno „Usklađenost sekundarnog prava Unije s pravom na zaštitu osobnih podataka").

4 Komisija je 10. siječnja 2017. podnijela prijedlog radi zamjene te direktive uredbom o privatnosti i elektroničkim komunikacijama.

5 Vijeće Europske unije odobrilo je 10. veljače 2021. pregovarački mandat radi izmjene pravila o zaštiti privatnosti i povjerljivosti u korištenju elektroničkih komunikacijskih usluga, kako bi se započeli pregovori s Europskim parlamentom. Tekst Prijedloga uredbe o poštovanju privatnog života i zaštiti osobnih podataka u elektroničkim komunikacijama te stavljanju izvan snage Direktive 2002/58/EZ (Uredba o privatnosti i elektroničkim komunikacijama) dostupan je na sljedećoj poveznici *https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_6087_2021_INIT&from=EN*.

6 Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (SL 2016., L 119, str. 1. i ispravci SL 2018., L 127, str. 2. i SL 2021., L 74, str. 35.)

kao i Direktivu (EU) 2016/680[7] o zaštiti navedenih podataka u kaznenim stvarima, čije se odredbe primjenjuju od 6. svibnja 2018.

Kad je riječ o obradi osobnih podataka u institucijama i tijelima Unije, njihova je zaštita osigurana, među ostalim, od 11. prosinca 2018. Uredbom (EU) 2018/1725[8]. U cilju usklađenog pristupa zaštiti osobnih podataka u cijeloj Uniji, tom se uredbom nastoje u najvećoj mogućoj mjeri uskladiti relevantna pravila u pogledu sustava uspostavljenog OUZP-om.

Naposljetku, kako bi se suočio s izazovima novih tehnologija, zakonodavac Unije 2020. pokrenuo je donošenje novih zakonodavnih mjera[9] povezanih s odredbama prava Unije o zaštiti osobnih podataka.

Uzimajući u obzir bogatu sudsku praksu Suda u području zaštite osobnih podataka, svrha je ovog tematskog prikaza predstaviti odabrane temeljne presude u tom području kao i presude koje su znatno doprinijele razvoju te sudske prakse, s posebnim naglaskom na presude koje je donijelo veliko vijeće Suda. Konkretnije, ovim se prikazom nastoji obuhvatiti sudska praksa koja se odnosi na opće propise u području zaštite osobnih podataka, koja proizlazi iz tumačenja Direktive 95/46 i OUZP-a, kao i sudska praksa koja se odnosi na sektorske propise, među ostalim, u sektoru elektroničkih komunikacija i kaznenog prava. Osim toga, njime se želi predstaviti izbor presuda koje se odnose na propise koji se primjenjuju horizontalno, pri čemu se prije svega naglašava odlučujuća uloga Povelje u razvoju sudske prakse.

---

7 Direktiva (EU) 2016/680 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka od strane nadležnih tijela u svrhe sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Okvirne odluke Vijeća 2008/977/PUP (SL 2016., L 119, str. 89. i ispravak SL 2018., L 127, str. 14.)

8 Uredba (EU) 2018/1725 Europskog parlamenta i Vijeća od 23. listopada 2018. o zaštiti pojedinaca u vezi s obradom osobnih podataka u institucijama, tijelima, uredima i agencijama Unije i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Uredbe (EZ) br. 45/2001 i Odluke br. 1247/2002/EZ (SL 2018., L 295, str. 39.).

9 U tom okviru, valja osobito istaknuti tri zakonodavne inicijative: *(i.)* Uredbu (EU) 2022/868 Europskog parlamenta i Vijeća od 30. svibnja 2022. o europskom upravljanju podacima i izmjeni Uredbe (EU) 2018/1724 (Akt o upravljanju podacima) (SL 2022., L 152, str. 1.) i Uredbu (EU) 2023/2854 Europskog parlamenta i Vijeća od 13. prosinca 2023. o usklađenim pravilima za pravedan pristup podacima i njihovu uporabu i o izmjeni Uredbe (EU) 2017/2394 i Direktive (EU) 2020/1828 (Akt o podacima) (SL 2023., L 2854, str. 1.); *(ii.)* zakonodavni paket o digitalnim uslugama i tržištima, koji se sastoji od Uredbe (EU) 2022/2065 Europskog parlamenta i Vijeća od 19. listopada 2022. o jedinstvenom tržištu digitalnih usluga i izmjeni Direktive 2000/31/EZ (Akt o digitalnim uslugama) (SL 2022., L 277, str. 1.) i Uredbe (EU) 2022/1925 Europskog parlamenta i Vijeća od 14. rujna 2022. o pravednim tržištima s mogućnošću neograničenog tržišnog natjecanja u digitalnom sektoru i izmjeni direktiva (EU) 2019/1937 i (EU) 2020/1828 (Akt o digitalnim tržištima) (SL 2022., L 265, str. 1.); i *(iii.)* prvi zakonodavni prijedlog čiji je cilj stvaranje regulatornog okvira za umjetnu inteligenciju, koji je konkretiziran Aktom o umjetnoj inteligenciji (SL 2024., L, 1689).

Sadržaj

I. Pravo na zaštitu osobnih podataka koje je priznato Poveljom Europske unije o temeljnim pravima

1. Usklađenost sekundarnog prava Unije s pravom na zaštitu osobnih podataka

Presuda od 9. studenoga 2010. (veliko vijeće), Volker und Markus Schecke i Eifert (C-92/09 i C-93/09,* EU:C:2010:662*)

U tom su predmetu u glavnom postupku bili suprotstavljeni poljoprivrednici i Land Hessen zbog objave njihovih osobnih podataka kao korisnika sredstava iz Europskog fonda za jamstva u poljoprivredi (EFJP) i Europskog poljoprivrednog fonda za ruralni razvoj (EPFRR) na internetskoj stranici Bundesanstalta für Landwirtschaft und Ernährung (Savezni ured za poljoprivredu i prehranu). Navedeni poljoprivrednici protivili su se takvoj objavi navodeći, među ostalim, da ona nije opravdana prevladavajućim javnim interesom. Land Hessen smatrao je da objava navedenih podataka proizlazi iz Uredbe (EZ) br. 1290/2005[10] i Uredbe (EZ) br. 259/2008[11], kojima je bilo uređeno financiranje zajedničke poljoprivredne politike i propisana objava informacija o pojedincima koji su korisnici EFJP-a i EPFRR-a.

U tom je kontekstu Verwaltungsgericht Wiesbaden (Upravni sud u Wiesbadenu, Njemačka) uputio Sudu nekoliko pitanja o valjanosti određenih odredbi Uredbe br. 1290/2005 i Uredbe br. 259/2008 kojima je propisana objava takvih informacija, među ostalim, na internetskim stranicama nacionalnih ureda.

Kad je riječ o uravnoteženosti prava na zaštitu osobnih podataka, koje je priznato Poveljom, i obveze transparentnosti u području europskih fondova, Sud navodi da je objava na internetskoj stranici osobnih podataka korisnika i iznosa koje su primili povreda njihova prava na zaštitu privatnog života općenito i prava na zaštitu njihovih osobnih podataka konkretno zbog toga što treći imaju slobodan pristup toj stranici.

Kako bi bila opravdana, takva povreda mora biti predviđena zakonom, poštovati bit navedenih prava i, primjenom načela proporcionalnosti, biti nužna i doista odgovarati ciljevima od općeg interesa koje priznaje Unija, pri čemu odstupanja od tih prava i njihova ograničenja moraju biti u granicama onoga što je krajnje nužno. Sud u tom kontekstu smatra da, iako u demokratskom društvu porezni obveznici imaju pravo biti

[10] Uredba Vijeća (EZ) br. 1290/2005 od 21. lipnja 2005. o financiranju zajedničke poljoprivredne politike (SL 2005., L 209, str. 1.) (SL, posebno izdanje na hrvatskom jeziku, poglavlje 14., svezak 1., str. 44.), koja je stavljena izvan snage Uredbom (EU) br. 1306/2013 Europskog parlamenta i Vijeća od 17. prosinca 2013. o financiranju, upravljanju i nadzoru zajedničke poljoprivredne politike (SL 2013., L 347, str. 549.)

[11] Uredba Komisije (EZ) br. 259/2008 od 18. ožujka 2008. o utvrđivanju detaljnih pravila za primjenu Uredbe Vijeća (EZ) br. 1290/2005 u pogledu objavljivanja informacija o korisnicima sredstava iz Europskog fonda za jamstva u poljoprivredi (EFJP) i Europskog poljoprivrednog fonda za ruralni razvoj (EPFRR) (SL 2008., L 76, str. 28.) (SL, posebno izdanje na hrvatskom jeziku, poglavlje 14., svezak 2., str. 182.), koja je stavljena izvan snage Provedbenom uredbom Komisije (EU) br. 908/2014 od 6. kolovoza 2014. o utvrđivanju pravila za primjenu Uredbe (EU) br. 1306/2013 Europskog parlamenta i Vijeća u pogledu agencija za plaćanja i ostalih tijela, financijskog upravljanja, poravnanja računa, pravila o kontroli, jamstava i transparentnosti (SL 2014., L 255, str. 59.)

informirani o uporabi javnih sredstava, Vijeće i Komisija ipak su dužni provesti uravnoteženo odvagivanje različitih predmetnih interesa, što prije donošenja spornih odredbi zahtijeva provjeru prekoračuje li objava države članice tih podataka na jednoj internetskoj stranici ono što je nužno za ostvarenje zadanih legitimnih ciljeva.

Sud stoga proglašava nevaljanima određene odredbe Uredbe br. 1290/2005 i Uredbu br. 259/2008 u cijelosti jer je tim odredbama u pogledu pojedinaca korisnika potpora EFJP-a i EPFRR-a bila propisana objava osobnih podataka o svim korisnicima, pri čemu se nije provodilo razlikovanje prema relevantnim kriterijima poput razdoblja tijekom kojih su oni primali takve potpore, njihovoj učestalosti odnosno vrsti i značaju. Međutim, Sud ne dovodi u pitanje učinke objave takvih popisa korisnika potpora koje su nacionalna tijela objavila u razdoblju prije objave presude.

Presuda od 8. travnja 2014. (veliko vijeće), Digital Rights Ireland i Seitlinger i dr. (spojeni predmeti C-293/12 i C-594/12*, EU:C:2014:238*)

Povod toj presudi bili su zahtjevi za ocjenu valjanosti Direktive 2006/24/EZ o zadržavanju podataka s obzirom na temeljna prava na poštovanje privatnog života i zaštitu osobnih podataka, koji su bili istaknuti u okviru nacionalnih sporova pred irskim odnosno austrijskim sudom. U glavnom postupku na koji se odnosio predmet C-293/12 High Court (Visoki sud, Irska) postupao je povodom spora između društva Digital Rights i irskih tijela u vezi sa zakonitošću nacionalnih mjera o zadržavanju podataka o elektroničkim komunikacijama. U glavnom postupku na koji se odnosio predmet C-594/12 Verfassungsgerichtshof (Ustavni sud, Austrija) postupao je povodom većeg broja ustavnih tužbi kojima se tražilo poništenje nacionalnog propisa kojim se Direktiva 2006/24 prenosila u austrijsko pravo.

Irski i austrijski sud svojim su zahtjevima za prethodnu odluku postavili Sudu upit o valjanosti Direktive 2006/24 s obzirom na članke 7., 8. i 11. Povelje. Preciznije, navedeni sudovi postavili su Sudu upit zadire li neopravdano u navedena temeljna prava obveza kojom se na temelju navedene direktive pružateljima javno dostupnih elektroničkih komunikacijskih usluga ili javnih komunikacijskih mreža nalaže da tijekom određenog razdoblja zadržavaju podatke o privatnom životu osobe i o njezinim komunikacijama te da nadležnim nacionalnim tijelima omogućuju pristup tim podacima. Predmetne vrste podataka obuhvaćaju, među ostalim, podatke koji su potrebni za pronalaženje i identifikaciju izvora i odredišta komunikacije, utvrđivanje datuma, vremena, trajanja i vrste komunikacije, komunikacijske opreme korisnikâ kao i za otkrivanje lokacije opreme za pokretnu komunikaciju, podatke o broju koji osobito sadržavaju ime i adresu pretplatnika ili registriranog korisnika, telefonski broj s kojeg se poziva i koji se poziva kao i adresu IP-a za internetske usluge. Ti podaci omogućavaju, među ostalim, saznanje s kojom je osobom pretplatnik ili registrirani korisnik komunicirao i kojim sredstvom kao i utvrđivanje vremena komunikacije te mjesta s kojeg se ona odvijala. Nadalje, oni omogućavaju uvid u učestalost komunikacija pretplatnika ili registriranog korisnika s određenim osobama tijekom danog razdoblja.

Sud prije svega navodi da su odredbe Direktive 2006/24, propisujući takve obveze tim pružateljima, osobito teško zadirale u temeljna prava na poštovanje privatnog života i zaštitu osobnih podataka, koja su zajamčena člancima 7. i 8. Povelje. U tom kontekstu Sud, doduše, smatra da bi se takvo zadiranje moglo opravdati ostvarivanjem cilja od općeg interesa, kao što je to borba protiv organiziranog kriminaliteta. Kao prvo, Sud navodi da zadržavanje podataka koje je propisano Direktivom nije moglo povrijediti bitan sadržaj temeljnih prava na poštovanje privatnog života i zaštitu osobnih podataka jer nije dopuštalo uvid u sadržaj elektroničke komunikacije kao takav i propisivalo je da pružatelji usluga ili mreža moraju poštovati određena načela zaštite i sigurnosti podataka. Kao drugo, Sud primjećuje da je zadržavanje podataka radi njihova mogućeg prenošenja nadležnim nacionalnim tijelima stvarno odgovaralo cilju od općeg interesa, odnosno borbi protiv teškog kriminaliteta, i, u konačnici, doprinosilo javnoj sigurnosti.

Međutim, Sud ocjenjuje da je zakonodavac Unije donošenjem Direktive o zadržavanju podataka prekoračio granice koje mu nalaže poštovanje načela proporcionalnosti. Stoga Sud Direktivu proglašava nevaljanom, smatrajući da njezino široko i osobito teško zadiranje u temeljna prava nije bilo dovoljno ograničeno kako bi se jamčilo da je to zadiranje ograničeno na ono što je krajnje nužno. Naime, Direktiva 2006/24 na općenit je način obuhvaćala svaku osobu i sva sredstva elektroničke komunikacije kao i sve podatke o prometu, bez ikakva razlikovanja, ograničenja ili iznimke s obzirom na cilj borbe protiv teških kaznenih djela. Nadalje, Direktivom nije bio predviđen nikakav objektivan kriterij koji bi omogućio jamstvo da nadležna nacionalna tijela imaju pristup podacima i mogućnost njihove uporabe samo u svrhu sprečavanja, otkrivanja ili kaznenog progona kaznenih djela koja se mogu smatrati dovoljno teškima za opravdanje takvog zadiranja niti je ona sadržavala materijalne i postupovne uvjete za takav pristup ili uporabu. Naposljetku, kad je riječ o trajanju zadržavanja podataka, Direktivom se propisivalo njihovo zadržavanje tijekom razdoblja koje nije kraće od šest mjeseci, a pritom se nije navodilo nikakvo razlikovanje između kategorija podataka s obzirom na osobe na koje se podaci odnose ili s obzirom na njihovu eventualnu korist za zadani cilj.

Osim toga, što se tiče zahtjeva koji proizlaze iz članka 8. stavka 3. Povelje, Sud utvrđuje da se Direktivom 2006/24 nisu predviđala dostatna jamstva koja bi omogućila učinkovitu zaštitu podataka od opasnosti zlouporabe, nezakonitog pristupa ili korištenja niti se propisivalo zadržavanje podataka na području Unije.

Posljedično, navedenom direktivom nije bio u potpunosti zajamčen nadzor neovisnog tijela poštovanja zahtjeva zaštite i sigurnosti, a kao što se to prema Povelji izričito zahtijeva.

Presuda od 21. lipnja 2022. (veliko vijeće), Ligue des droits humains (C-817/19, EU:C:2022:491)

Podaci iz PNR-a (*Passenger Name Record*) informacije su o rezervaciji koje pohranjuju zračni prijevoznici u svojim sustavima rezervacija i kontrole odlazaka. Direktiva o PNR-u[12] obvezuje te prijevoznike da podatke o svim putnicima koji putuju na letu između EU-a i trećih zemalja prenesu odjelu za informacije o putnicima (u daljnjem tekstu: PIU) države članice odredišta ili polaska predmetnog leta u svrhu borbe protiv kaznenih djela terorizma i teških kaznenih djela. Naime, u pogledu tako prenesenih podataka iz PNR-a PIU provodi prethodnu procjenu[13] te se oni zatim čuvaju u svrhu eventualne naknadne procjene koju provode nadležna tijela dotične države članice ili druge države članice. Države članice mogu odlučiti primijeniti Direktivu i na letove unutar EU-a[14].

Ligue des droits humains podnio je Couru constitutionnelle (Ustavni sud, Belgija) tužbu za poništenje protiv belgijskog zakona kojim se u nacionalno pravo prenosi kako Direktiva o PNR-u tako i Direktiva o API-ju[15]. Prema tužiteljevu mišljenju, tim se zakonom povređuje pravo na poštovanje privatnog života i zaštitu osobnih podataka. Tužitelj kritizira, s jedne strane, široki opseg podataka iz PNR-a i, s druge strane, opću prirodu prikupljanja, prijenosa i obrade tih podataka. Zakonom se ugrožava i slobodno kretanje osoba jer se njime neizravno ponovno uspostavljaju granične kontrole proširenjem PNR sustava na letove unutar EU-a i prijevoze koji se odvijaju drugim sredstvima unutar Unije.

U tom kontekstu, belgijski Cour constitutionnelle (Ustavni sud) uputio je Sudu zahtjev za prethodnu odluku o pitanjima koja se odnose, među ostalim, na valjanost Direktive o PNR-u.

Sud u presudi koju je donijelo njegovo veliko vijeće potvrđuje valjanost Direktive o PNR-u jer se ona može tumačiti u skladu s Poveljom.

Sud u tom pogledu odlučuje da, s obzirom na to da se tumačenjem koje je Sud utvrdio u pogledu odredbi Direktive o PNR-u u vezi s temeljnim pravima zajamčenim člancima 7., 8. i 21. te člankom 52. stavkom 1. Povelje[16] osigurava usklađenost te direktive s tim člancima, razmatranjem upućenih pitanja nije utvrđen nijedan element koji može utjecati na valjanost navedene direktive.

---

12 Direktiva (EU) 2016/681 Europskog parlamenta i Vijeća od 27. travnja 2016. o uporabi podataka iz evidencije podataka o putnicima (PNR) u svrhu sprečavanja, otkrivanja, istrage i kaznenog progona kaznenih djela terorizma i teških kaznenih djela (SL 2016., L 119, str. 132. i ispravak SL 2021., L 137, str. 20., u daljnjem tekstu: Direktiva o PNR-u)

13 Cilj je te procjene identificirati osobe koje bi nadležna tijela trebala dodatno ispitati s obzirom na to da bi te osobe mogle biti uključene u kazneno djelo terorizma ili teško kazneno djelo. Provodi se na sustavan i automatiziran način, uspoređivanjem podataka iz PNR-a s „relevantnim" bazama podataka ili njihovom obradom s obzirom na kriterije koji su prethodno utvrđeni člankom 6. stavkom 2. točkom (a) i člankom 6. stavkom 3. Direktive o PNR-u.

14 Time koriste mogućnost predviđenu u članku 2. Direktive o PNR-u.

15 Direktiva Vijeća 2004/82/EZ od 29. travnja 2004. o obvezi prijevoznika na dostavljanje podataka o putnicima (SL 2004., L 261, str. 24.) (SL, posebno izdanje na hrvatskom jeziku, poglavlje 19., svezak 8., str. 77., u daljnjem tekstu: Direktiva o API-ju). Tom se direktivom propisuje da zračni prijevoznici nadležnim nacionalnim tijelima prenose informacije o putnicima koje će prevoziti (kao što su broj i vrsta putnog dokumenta koji se koristi te nacionalnost), s ciljem poboljšanja graničnih kontrola i sprečavanja nezakonitog useljavanja.

16 U skladu s tom odredbom, svako ograničenje pri ostvarivanju prava i sloboda priznatih Poveljom mora biti predviđeno zakonom i mora poštovati njihovu bit. Usto, ograničenja tih prava i sloboda moguća su samo ako su potrebna i ako zaista odgovaraju ciljevima u općem interesu koje priznaje Unija ili potrebi zaštite prava i sloboda drugih osoba.

Uvodno, Sud podsjeća na to da se akt Unije mora tumačiti, u najvećoj mogućoj mjeri, tako da se ne dovede u pitanje njegova valjanost i u skladu s cjelokupnim primarnim pravom i osobito odredbama Povelje, a države članice stoga trebaju osigurati da se ne oslanjaju na njegovo tumačenje koje bi bilo u sukobu s temeljnim pravima zaštićenima pravnim poretkom Unije ili drugim općim načelima priznatima u tom pravnom poretku. Što se tiče Direktive o PNR-u Sud pojašnjava da se velikim brojem njezinih uvodnih izjava i odredbi zahtijeva takvo usklađeno tumačenje, pri čemu se naglašava važnost koju zakonodavac Unije, kad upućuje na veću razinu zaštite podataka, pridaje punom poštovanju temeljnih prava propisanih Poveljom.

Sud utvrđuje da Direktiva o PNR-u sadržava nedvojbeno ozbiljna zadiranja u prava zajamčena člancima 7. i 8. Povelje, osobito u dijelu u kojem se njome nastoji uspostaviti sustav stalnog, neciljanog i sustavnog nadzora koji uključuje automatiziranu procjenu osobnih podataka svih osoba koje se koriste uslugama zračnog prijevoza. Podsjeća na to da mogućnost država članica da opravdaju takvo zadiranje treba ocijeniti tako da se odmjeri njegova ozbiljnost i provjeri da je važnost cilja od općeg interesa koji se nastoji postići proporcionalna toj ozbiljnosti.

Sud zaključuje kako se može smatrati da su prijenos, obrada i čuvanje podataka iz PNR-a koji su predviđeni tom direktivom ograničeni na ono što je strogo nužno u svrhu borbe protiv kaznenih djela terorizma i teških kaznenih djela, pod uvjetom da se ovlasti predviđene navedenom direktivom usko tumače. U tom pogledu, u ovoj se presudi navodi, među ostalim, sljedeće:

- Sustav uspostavljen Direktivom o PNR-u smije obuhvaćati samo informacije koje su jasno odredive i ograničene u rubrikama u Prilogu I. toj direktivi i koje su povezane s izvedenim letom i dotičnim putnikom, što za neke rubrike u tom prilogu znači da su obuhvaćene samo informacije koje se u njima izričito navode[17].

- Primjenu sustava uspostavljenog Direktivom o PNR-u treba ograničiti na kaznena djela terorizma i samo na teška kaznena djela koja su, makar i posredno, objektivno povezana sa zračnim prijevozom putnika. Što se tiče tih teških kaznenih djela, primjena tog sustava ne može se proširiti na kaznena djela koja, iako ispunjavaju kriterij predviđen tom direktivom koji se odnosi na stupanj težine te se osobito navode u Prilogu II. toj direktivi, ulaze u okvir standardnih kaznenih djela, s obzirom na posebnosti nacionalnog kaznenog sustava.

- Eventualno proširenje primjene Direktive o PNR-u na sve ili dio letova unutar EU-a, koje država članica može odlučiti primijeniti iskorištavanjem mogućnosti predviđene tom direktivom, treba ograničiti na ono što je strogo nužno. U tu svrhu, sud ili neovisno upravno tijelo mora moći provesti djelotvoran nadzor u

[17] Prema tome, među ostalim, „podaci o načinu plaćanja" (rubrika 6. Priloga) smiju se odnositi samo na načine plaćanja i izdavanje računa za zrakoplovnu kartu, pri čemu su isključene sve ostale informacije koje nisu izravno povezane s letom, a „opće primjedbe» (rubrika 12.) mogu se odnositi samo na informacije izričito navedene u toj rubrici, koje se odnose na maloljetne putnike.

pogledu te primjene na način da odluka tog suda odnosno tijela ima obvezujući učinak. U tom pogledu Sud pojašnjava da:

- Samo u situaciji u kojoj navedena država članica utvrdi da postoje dovoljno konkretne okolnosti zbog kojih se može smatrati da je suočena s ozbiljnom terorističkom prijetnjom koja se pokaže stvarnom i trenutačnom ili predvidljivom, primjena te direktive na sve letove unutar EU-a s polazištem ili odredištem u navedenoj državi članici na razdoblje koje je ograničeno na ono što je strogo nužno, ali se može obnoviti, ne prekoračuje granice onoga što je strogo nužno[18].

- Ako takva teroristička prijetnja ne postoji, primjena navedene direktive ne može se proširiti na sve letove unutar EU-a, nego je treba ograničiti na letove unutar EU-a koji se osobito odnose na određene zračne linije ili obrasce putovanja ili pak određene zračne luke za koje, u skladu s ocjenom dotične države članice, postoje naznake koje mogu opravdati tu primjenu. Strogo nužnu prirodu te primjene na tako odabrane letove unutar EU-a treba redovito preispitivati s obzirom na promjenu uvjeta koji opravdavaju njezin odabir.

- Za potrebe prethodne procjene podataka iz PNR-a, čiji je cilj identificirati osobe za koje je potrebno dodatno ispitivanje prije njihova dolaska ili odlaska te koju se najprije provodi automatiziranom obradom, PIU može, s jedne strane, usporediti te podatke samo s bazama podataka koje se odnose na osobe ili predmete koji se traže ili za koje postoji upozorenje[19]. Te baze podataka trebaju biti nediskriminirajuće te ih nadležna tijela trebaju upotrebljavati za borbu protiv kaznenih djela terorizma i teških kaznenih djela koja su, makar i posredno, objektivno povezana sa zračnim prijevozom putnika. S druge strane, što se tiče prethodne procjene s obzirom na prethodno utvrđene kriterije, PIU ne može upotrebljavati tehnologije umjetne inteligencije u okviru sustava za samostalno učenje (*machine learning*), koji bez ljudske intervencije i kontrole mogu izmijeniti postupak procjene i, konkretno, kriterije procjene na kojima se temelji rezultat primjene tog postupka, kao i ponderiranje tih kriterija. Navedene kriterije treba odrediti tako da je njihova primjena posebno usmjerena na pojedince u pogledu kojih može postojati osnovana sumnja da su sudjelovali u kaznenim djelima terorizma ili teškim kaznenim djelima i tako da se uzmu u obzir elementi koji se

[18] Naime, postojanje takve opasnosti može samo po sebi uspostaviti vezu između prijenosa i obrade predmetnih podataka te borbe protiv terorizma. Prema tome, predviđanje primjene Direktive o PNR-u na sve letove unutar EU-a s polazištem ili odredištem u dotičnoj državi članici na određeno razdoblje ne prekoračuje granice onoga što je strogo nužno jer sud ili neovisno upravno tijelo mora moći provesti nadzor u pogledu odluke kojom se predviđa ta primjena.

[19] Odnosno s bazama podataka koje se odnose na osobe ili predmete koji se traže ili za koje postoji upozorenje u smislu članka 6. stavka 3. točke (a) Direktive o PNR-u. Suprotno tomu, analize na temelju različitih baza podataka mogu imati oblik rudarenja podataka (*data mining*) te dovesti do nerazmjerne uporabe tih podataka i pružiti sredstva za određivanje detaljnog profila dotičnih osoba samo zato što namjeravaju putovati zrakoplovom.

nekome „stavljaju na teret” i oni koji mu „idu u korist”, pri čemu ne smije postojati izravna ili neizravna diskriminacija[20].

- S obzirom na stopu pogreške specifičnu za takvu automatiziranu obradu podataka iz PNR-a i na prilično velik broj „lažnih pozitivnih” rezultata dobivenih nakon njezine primjene tijekom 2018. i 2019., prikladnost sustava uspostavljenog Direktivom o PNR-u da ostvari postavljene ciljeve u biti ovisi o dobrom funkcioniranju neautomatizirane provjere pozitivnih rezultata dobivenih tom obradom, koju naknadno provodi PIU. U tom pogledu, države članice trebaju predvidjeti jasna i precizna pravila u skladu s kojima će se voditi i usmjeravati analiza koju provode službenici PIU-a zaduženi za tu pojedinačnu provjeru kako bi se osiguralo puno poštovanje temeljnih prava propisanih člancima 7., 8. i 21. Povelje i, osobito, kako bi se zajamčila dosljedna upravna praksa u okviru PIU-a kojom se poštuje načelo nediskriminacije. Konkretno, one trebaju osigurati da PIU utvrdi objektivne kriterije provjere na temelju kojih njegovi službenici mogu provjeriti, s jedne strane, odnosi li se stvarno i u kojoj mjeri pozitivni rezultat (hit) na pojedinca koji bi mogao biti uključen u kaznena djela terorizma ili teška kaznena djela te, s druge strane, nediskriminirajuću prirodu automatizirane obrade. U tom kontekstu, Sud naglašava i da nadležna tijela trebaju osigurati da zainteresirana osoba može razumjeti funkcioniranje prethodno utvrđenih kriterija procjene i programa koji primjenjuju te kriterije, tako da može odlučiti uz potpuno poznavanje činjenica hoće li ostvariti svoje pravo na podnošenje pravnog sredstva. Isto tako, u okviru takvog pravnog sredstva, sud zadužen za nadzor zakonitosti odluke koju su donijela nadležna tijela, kao i, osim u slučajevima prijetnji državnoj sigurnosti, sama zainteresirana osoba moraju se moći upoznati sa svim razlozima i dokazima na temelju kojih je ta odluka donesena, uključujući prethodno utvrđene kriterije procjene i funkcioniranje programa koji primjenjuju te kriterije.

- Naknadno dostavljanje i procjena podataka iz PNR-a, odnosno nakon dolaska ili polaska dotične osobe, mogu se provesti samo na temelju novih okolnosti i objektivnih elemenata koji su takve prirode da mogu ukazivati na postojanje osnovane sumnje da je ta osoba uključena u teška kaznena djela koja su, makar i posredno, objektivno povezana sa zračnim prijevozom putnika ili na temelju kojih se može smatrati da ti podaci u konkretnom slučaju mogu dati stvaran doprinos borbi protiv kaznenih djela terorizma koja imaju takvu vezu. Dostavljanju podataka iz PNR-a u svrhu takve naknadne procjene, osim u propisno opravdanom hitnom slučaju, u načelu treba prethoditi nadzor suda ili neovisnog upravnog tijela, koji se provodi na obrazloženi zahtjev nadležnih tijela, i to

[20] Prethodno utvrđeni kriteriji moraju biti usmjereni, proporcionalni i određeni te ih treba redovito preispitivati (članak 6. stavak 4. Direktive o PNR-u). Prethodnu procjenu s obzirom na prethodno utvrđene kriterije treba provesti na nediskriminirajući način. U skladu s člankom 6. stavkom 4. četvrtom rečenicom Direktive o PNR-u, kriteriji se ni u kojem slučaju ne smiju temeljiti na rasnom ili etničkom podrijetlu osobe, njezinim političkim mišljenjima, vjeri ili filozofskim uvjerenjima, članstvu u sindikatu, zdravstvenom stanju, seksualnom životu ili spolnoj orijentaciji.

neovisno o tome je li taj zahtjev podnesen prije ili poslije isteka roka od šest mjeseci nakon prijenosa tih podataka PIU-u[21].

Presuda od 22. studenoga 2022. (veliko vijeće), Luxembourg Business Registers (C-37/20 i C-601/20, EU:C:2022:912)

U svrhu borbe protiv pranja novca i financiranja terorizma kao i u svrhu sprečavanja takvih ponašanja, Direktiva o sprečavanju pranja novca[22] nalaže državama članicama da osnuju registar koji sadržava informacije o stvarnim vlasnicima[23] korporativnih i drugih pravnih subjekata osnovanih na njihovim područjima. Nakon izmjene navedene direktive Direktivom 2018/843[24], neke od tih informacija moraju biti u svim slučajevima dostupne cjelokupnoj javnosti. U skladu s tako izmijenjenom Direktivom o sprečavanju pranja novca (u daljnjem tekstu: izmijenjena Direktiva o sprečavanju pranja novca), luksemburškim zakonodavstvom osnovan je Registar stvarnih vlasnika (u daljnjem tekstu: RSV) čija je svrha čuvanje i stavljanje na raspolaganje niza informacija o stvarnim vlasnicima registriranih subjekata, a kojem može pristupiti cjelokupna javnost.

U tim okolnostima, pred tribunalom d'arrondissement de Luxembourg (Općinski sud u Luxembourgu, Luksemburg) pokrenuta su dva postupka, koja su pokrenuli osoba WM i društvo Sovim SA, povodom odbijanja Luxembourg Business Registersa, upravitelja RSV-a, njihovih zahtjeva za sprečavanje pristupa cjelokupne javnosti podacima koji se odnose, u prvom predmetu, na svojstvo osobe WM kao stvarnog vlasnika jednog društva za poslovanje nekretninama i, u drugom predmetu, na stvarnog vlasnika društva Sovim SA. U okviru tih dvaju predmeta tribunal d'arrondissement de Luxembourg (Općinski sud u Luxembourgu), sumnjajući posebice u valjanost odredbi prava Unije kojima se osniva sustav pristupa javnosti informacijama o stvarnim vlasnicima, uputio je Sudu prethodno pitanje o ocjeni valjanosti odredbi prava Unije.

Svojom presudom Sud, odlučujući u velikom vijeću, utvrđuje nevaljanost Direktive 2018/843 u dijelu u kojem je njome izmijenjena Direktiva o pranju novca na način da države članice moraju osigurati da su informacije o stvarnom vlasništvu korporativnih i drugih pravnih subjekata osnovanih na njihovu državnom području u svim slučajevima dostupne cjelokupnoj javnosti[25].

Na prvome mjestu, Sud utvrđuje da pristup cjelokupne javnosti podacima o stvarnim vlasnicima predviđen Direktivom o sprečavanju pranja novca predstavlja ozbiljno

---

21 U skladu s člankom 12. stavcima 1. i 3. Direktive o PNR-u, takav se nadzor izričito predviđa samo za zahtjeve za dostavu podataka iz PNR-a koji su podneseni nakon isteka roka od šest mjeseci od prijenosa tih podataka PIU-u.

22 Direktiva (EU) 2015/849 Europskog parlamenta i Vijeća od 20. svibnja 2015. o sprečavanju korištenja financijskog sustava u svrhu pranja novca ili financiranja terorizma, o izmjeni Uredbe (EU) br. 648/2012 Europskog parlamenta i Vijeća te o stavljanju izvan snage Direktive 2005/60/EZ Europskog parlamenta i Vijeća i Direktive Komisije 2006/70/EZ (SL 2015., L 141, str. 73., u daljnjem tekstu: Direktiva o sprečavanju pranja novca)

23 U skladu s člankom 3. točkom 6. Direktive o sprečavanju pranja novca, stvarni vlasnik znači fizička osoba koja u konačnici posjeduje ili kontrolira stranku i/ili fizička osoba ili više njih u čije ime se provodi transakcija.

24 Direktiva (EU) 2018/843 Europskog parlamenta i Vijeća od 30. svibnja 2018. o izmjeni Direktive (EU) 2015/849 o sprečavanju korištenja financijskog sustava u svrhu pranja novca ili financiranja terorizma i o izmjeni direktiva 2009/138/EZ i 2013/36/EU (SL 2018., L 156, str. 43.)

25 Nevaljanost članka 1. točke 15. podtočke (c) Direktive 2018/843, kojim se mijenja članak 30. stavak 5. prvi podstavak točka (c) Direktive o sprečavanju pranja novca

zadiranje u temeljna prava na zaštitu privatnog života i na zaštitu osobnih podataka, koja su utvrđena člancima 7. i 8. Povelje.

U tom pogledu Sud navodi da, budući da predmetni podaci sadržavaju informacije o fizičkim osobama čiji je identitet utvrđen, to jest stvarnim vlasnicima korporativnih i drugih pravnih subjekata osnovanih na području država članica, pristupom cjelokupne javnosti tim podacima zadire se u temeljno pravo na poštovanje privatnog života. Usto, takvo stavljanje na raspolaganje cjelokupnoj javnosti navedenih podataka predstavlja obradu osobnih podataka. Sud dodaje da takvo stavljanje na raspolaganje cjelokupnoj javnosti predstavlja zadiranje u dva navedena temeljna prava, neovisno o kasnijem korištenju dostavljenim informacijama.

Kada je riječ o ozbiljnosti tog zadiranja, Sud ističe da, kada se informacije stavljene na raspolaganje cjelokupnoj javnosti odnose na identitet stvarnog vlasnika kao i na prirodu i opseg vlasničkih udjela koje drži u društvima ili drugim pravnim subjektima, one mogu omogućiti izradu profila koji se odnosi na određene osobne identifikacijske podatke, imovinsko stanje dotične osobe kao i gospodarske sektore, države i konkretna poduzeća u koje je ona ulagala. Usto, te informacije postaju dostupne potencijalno neograničenom broju osoba, tako da takva obrada osobnih podataka može osobama koje se – zbog razloga koji nemaju veze s ciljem koji se ostvaruje tom mjerom – pokušavaju informirati posebice o materijalnoj i financijskoj situaciji stvarnog vlasnika omogućiti slobodan pristup tim podacima. Ta je mogućnost još i jednostavnija kada se predmetni podaci mogu konzultirati na internetu. Usto, potencijalne posljedice za dotične osobe koje proizlaze iz eventualne zlouporabe njihovih osobnih podataka pogoršane su činjenicom da, kada se jednom stave na raspolaganje cjelokupnoj javnosti, te podatke ne samo da je moguće slobodno konzultirati, već ih je moguće i spremiti i distribuirati, te da u tom slučaju postaje još teže, pa čak i nemoguće, da se te osobe učinkovito brane od zlouporaba.

Na drugome mjestu, prilikom ispitivanja opravdanja predmetnog zadiranja Sud primjećuje da je u ovom predmetu poštovano načelo zakonitosti. Naime, ograničavanje ostvarivanja prethodno navedenih temeljnih prava koje proizlazi iz pristupa cjelokupne javnosti informacijama o stvarnim vlasnicima predviđeno je zakonodavnim aktom, odnosno izmijenjenom Direktivom o sprečavanju pranja novca. Usto, s jedne strane, ta direktiva precizira da ti podaci moraju biti odgovarajući, točni i ažurirani te se izrijekom nabrajaju neki od tih podataka kojima cjelokupna javnost mora imati pristup. S druge strane, njome se utvrđuju uvjeti pod kojima države članice mogu predvidjeti izuzeća od takvog pristupa.

Kao drugo, Sud pojašnjava da predmetno zadiranje ne ugrožava bitni sadržaj temeljnih prava zajamčenih člancima 7. i 8. Povelje. Iako je točno da Direktiva o sprečavanju pranja novca ne sadržava taksativno navođenje podataka kojima cjelokupna javnost mora imati pristup i da su države članice ovlaštene da omoguće pristup dodatnim informacijama, činjenica je da se samo odgovarajuće informacije o stvarnim vlasnicima i vlasničkim udjelima koje drže mogu pribaviti i čuvati te – posljedično – potencijalno učiniti dostupnima javnosti, što isključuje, među ostalim, informacije koje nemaju odgovarajući odnos s ciljevima te direktive. Međutim, ne proizlazi da bi stavljanje na raspolaganje

cjelokupnoj javnosti informacija koje imaju takav odnos nekako ugrozilo bitan sadržaj navedenih temeljnih prava.

Kao treće, Sud ističe da zakonodavac Unije, time što predviđa pristup cjelokupne javnosti informacijama o stvarnim vlasnicima, želi spriječiti pranje novca i financiranje terorizma, na način da povećanom transparentnosti stvara okruženje za koje je manje vjerojatno da će biti korišteno u te svrhe, što predstavlja cilj u općem interesu kojim se može opravdati zadiranje, čak i ozbiljno, u temeljna prava priznata člancima 7. i 8. Povelje.

Kao četvrto, u okviru ispitivanja prikladnosti, nužnosti i proporcionalnosti predmetnog zadiranja, Sud utvrđuje da je točno da je pristup cjelokupne javnosti informacijama o stvarnim korisnicima prikladan da doprinese ostvarenju tog cilja.

Međutim, on smatra da se ne može smatrati da je to zadiranje ograničeno na ono što je nužno. S jedne strane, stroga nužnost tog zadiranja ne može se dokazati pozivajući se na činjenicu da je kriterij „legitimnog interesa" koji, prema Direktivi o sprečavanju pranja novca u njezinoj verziji prije izmjene putem Direktive 2018/843, mora imati svatko tko želi pristupiti informacijama o stvarnim vlasnicima, teško primijeniti i da njegova primjena može dovesti do proizvoljnih odluka. Naime, moguće postojanje poteškoća za precizno utvrđivanje slučajeva i uvjeta u kojima javnost može pristupiti informacijama o stvarnim korisnicima ne može opravdati to da zakonodavac Unije predvidi pristup cjelokupne javnosti tim informacijama.

S druge strane, niti objašnjenja koja se nalaze u Direktivi 2018/843 ne mogu dokazati strogu nužnost predmetnog zadiranja[26]. U mjeri u kojoj se, prema tim objašnjenjima, pristupom cjelokupne javnosti informacijama o stvarnom vlasništvu civilnom društvu, posebice tisku i udrugama civilnog društva, treba omogućiti bolja kontrola nad informacijama, Sud ističe da kako tisak tako i udruge civilnog društva koje imaju poveznicu sa sprečavanjem i borbom protiv pranja novca i financiranja terorizma imaju legitimni interes da pristupe informacijama o stvarnim vlasnicima. Isto vrijedi i u pogledu osoba koje žele znati identitet stvarnih vlasnika društva ili drugog pravnog subjekta zbog toga što s njim mogu sudjelovati u transakcijama ili pak u pogledu financijskih institucija i tijela koja sudjeluju u borbi protiv kaznenih djela u području pranja novca ili financiranja terorizma.

Osim toga, predmetno zadiranje nije ni proporcionalno. U tom pogledu Sud utvrđuje da materijalna pravila kojima se uređuje to zadiranje ne udovoljavaju zahtjevu jasnoće i preciznosti. Naime, izmijenjena Direktiva o sprečavanju pranja novca predviđa da cjelokupna javnost ima pristup „barem" podacima iz te odredbe te državama članicama daje mogućnost da omoguće pristup dodatnim informacijama koje uključuju „barem" informacije o datumu rođenja ili podatke za kontakt predmetnog stvarnog vlasnika. No, uporabom izraza „barem" ta direktiva dopušta stavljanje na raspolaganje javnosti podataka koji nisu u dovoljnoj mjeri definirani niti utvrdivi.

[26] Misli se na objašnjenja koja se nalaze u uvodnoj izjavi 30. Direktive 2018/843.

Osim toga, kad je riječ o odvagivanju ozbiljnosti tog zadiranja s važnošću cilja u općem interesu koji se želi ostvariti, Sud priznaje da, s obzirom na njegovu važnost, taj cilj može opravdati zadiranja, čak i ozbiljna, u temeljna prava utvrđena u člancima 7. i 8. Povelje.

Međutim, s jedne strane, borba protiv pranja novca i financiranja terorizma je ponajprije dužnost javnih tijela i subjekata, kao što su kreditne i financijske institucije, kojima su, zbog njihovih aktivnosti, nametnute posebne obveze u tom području. Zbog toga izmijenjena Direktiva o sprečavanju pranja novca predviđa da su informacije o stvarnom vlasništvu u svim slučajevima dostupne nadležnim tijelima i financijsko-obavještajnim jedinicama bez ikakva ograničenja, kao i obveznicima, u okviru dubinske analize stranaka[27].

S druge strane, u usporedbi s prethodnim sustavom, koji je predviđao, osim pristupa nadležnih tijela i određenih subjekata, i pristup svih osoba ili organizacija koje mogu dokazati legitimni interes, sustav koji je uveden Direktivom 2018/843 predstavlja značajno ozbiljniju povredu temeljnih prava zajamčenih člancima 7. i 8. Povelje a da to pogoršanje nije kompenzirano eventualnim koristima koje bi mogle proizlaziti iz potonjeg sustava u odnosu na prethodni, što se tiče borbe protiv pranja novca i financiranja terorizma.

2. Poštovanje prava na zaštitu osobnih podataka u provedbi prava Unije

Presuda od 21. prosinca 2016. (veliko vijeće), Tele2 Sverige (spojeni predmeti C-203/15 i C-698/15, EU:C:2016:970)

Nakon što je presudom Digital Rights Ireland i Seitlinger i dr. Direktiva 2006/24 proglašena nevaljanom (vidjeti *supra*), Sud je postupao u dvama predmetima koji su se odnosili na opću obvezu propisanu pružateljima elektroničkih komunikacijskih usluga u Švedskoj i Ujedinjenoj Kraljevini da zadržavaju podatke o tim komunikacijama, pri čemu je to zadržavanje bilo predviđeno direktivom koja je proglašena nevaljanom.

Dan nakon objave presude Digital Rights Ireland i Seitlinger i dr., telekomunikacijsko poduzeće Tele2 Sverige obavijestilo je švedsko tijelo za nadzor pošte i telekomunikacija o svojoj odluci da prestaje zadržavati podatke i namjeri uklanjanja podataka koji su do tada zadržani (predmet C-203/15). Naime, švedskim pravom obvezivalo se pružatelje elektroničkih komunikacijskih usluga da sustavno i stalno, i to bez bilo kakve iznimke, zadržavaju podatke o prometu i lokaciji svih pretplatnika i registriranih korisnika u pogledu svih sredstava elektroničke komunikacije. U predmetu C-698/15 tri su osobe podnijele tužbe protiv britanskog sustava zadržavanja podataka koji je ovlašćivao ministra unutarnjih poslova da javnim telekomunikacijskim operatorima nalaže

[27] Članak 30. stavak 5. prvi podstavak točke (a) i (b) izmijenjene Direktive o sprečavanju pranja novca

zadržavanje svih komunikacijskih podataka u trajanju od najviše dvanaest mjeseci, pri čemu je zadržavanje sadržaja tih komunikacija ipak bilo isključeno.

Postupajući povodom zahtjeva Kammarrättena i Stockholm (Žalbeni upravni sud u Stockholmu, Švedska) i Courta of Appeal (England & Wales) (Civil Division) (Žalbeni sud, Engleska i Wales, Građanski odjel, Ujedinjena Kraljevina), Sud je bio pozvan donijeti odluku o tumačenju članka 15. stavka 1. Direktive 2002/58 o privatnosti i elektroničkim komunikacijama, kojim se državama članicama omogućavalo da uvedu određene iznimke od obveze, propisane tom direktivom, da osiguraju povjerljivost elektroničkih komunikacija i s time povezanih podataka o prometu.

Sud u svojoj presudi prije svega presuđuje da se članku 15. stavku 1. Direktive 2002/58, u vezi s člancima 7., 8. i 11. kao i člankom 52. stavkom 1. Povelje, protivi nacionalni propis poput onoga u Švedskoj, koji u cilju borbe protiv kriminaliteta određuje opće i neselektivno zadržavanje svih podataka o prometu i lokaciji svih pretplatnika i registriranih korisnika u pogledu svih sredstava elektroničke komunikacije. Sud smatra da takav propis prelazi granice krajnje nužnog i ne može se smatrati opravdanim u demokratskom društvu, kao što se to zahtijeva navedenim člankom 15. stavkom 1., u vezi s gore navedenim člancima Povelje.

Toj istoj odredbi u vezi s istim člancima Povelje protivi se nacionalni propis kojim se uređuje zaštita i sigurnost podataka o prometu i lokaciji i osobito pristup nadležnih nacionalnih tijela zadržanim podacima kad svrha tog pristupa u okviru borbe protiv kriminaliteta nije ograničena na borbu protiv teških kaznenih djela, kad se navedeni pristup ne podvrgava prethodnom nadzoru suda ili neovisnog upravnog tijela i kad nije propisano da se predmetni podaci zadržavaju na području Unije.

Nasuprot tomu, Sud smatra da se članku 15. stavku 1. Direktive 2002/58 ne protivi propis koji radi prevencije omogućava ciljano zadržavanje takvih podataka u svrhu borbe protiv teških kaznenih djela, pod uvjetom da to zadržavanje bude ograničeno na ono što je krajnje nužno kad je riječ o kategorijama podataka koji trebaju biti zadržani, predviđenim komunikacijskim sredstvima, osobama na koje se zadržavanje odnosi kao i njegovu trajanju. Kako bi bili ispunjeni ti zahtjevi, taj nacionalni propis mora, kao prvo, odrediti jasna i precizna pravila koja omogućuju učinkovitu zaštitu podataka od opasnosti zlouporabe. On mora osobito naznačiti okolnosti i uvjete u kojima mjera zadržavanja podataka može biti preventivno donesena, jamčeći pritom njezino ograničavanje na ono što je krajnje nužno. Kao drugo, kad je riječ o materijalnim uvjetima koje mora ispuniti nacionalni propis kako bi se osiguralo da bude ograničen na ono što je krajnje nužno, zadržavanje podataka mora uvijek ispunjavati objektivne kriterije, uspostavljajući vezu između podataka koje treba zadržati i zadanog cilja. Takvi uvjeti moraju se u praksi pokazati takvima da mogu učinkovito ograničiti doseg mjere i stoga javnost na koju se ona odnosi. Kad je riječ o tom ograničenju, nacionalni propis mora se temeljiti na objektivnim kriterijima koji omogućuju obuhvaćanje javnosti čiji podaci mogu otkriti vezu, makar i posrednu, s teškim kaznenim djelima, doprinošenje na bilo koji način borbi protiv teških kaznenih djela ili sprečavanje ozbiljne opasnosti za javnu sigurnost.

II. Obrada osobnih podataka u smislu općih propisa u tom području

1. Područje primjene općih propisa

Presuda od 30. svibnja 2006. (veliko vijeće), Parlament/Vijeće (C-317/04 i C-318/04, EU:C:2006:346)

Nakon terorističkih napada 11. rujna 2001., Sjedinjene Američke Države donijele su zakonodavstvo kojim su zračni prijevoznici koji osiguravaju letove čije je odredište ili polazište državno područje SAD-a odnosno letove koji prelaze preko njega dužni tijelima SAD-a pružiti elektronički pristup podacima iz svojih sustava za rezervaciju i nadzor polazaka, naziva *Passenger Name Records* (PNR).

Smatrajući da bi te odredbe mogle doći u sukob s europskim zakonodavstvom i zakonodavstvom država članica u području zaštite podataka, Komisija je započela pregovore s tijelima SAD-a. Nakon završetka tih pregovora, Komisija je 14. svibnja 2004. donijela Odluku 2004/535/EZ[28] kojom se utvrđuje da Ured za carinsku i graničnu zaštitu SAD-a (United States Bureau of Customs and Border Protection, u daljnjem tekstu: CBP) osigurava odgovarajuću razinu zaštite podataka iz PNR-a koji se prenose iz Zajednice (u daljnjem tekstu: odluka o odgovarajućoj razini zaštite podataka). Vijeće je zatim 17. svibnja 2004. donijelo Odluku 2004/496/EZ[29] kojom se odobrava sklapanje Sporazuma između Europske zajednice i SAD-a o obradi i prijenosu podataka iz PNR-a zračnih prijevoznika s poslovnim nastanom na državnom području država članica Zajednice CBP-u.

Europski parlament zatražio je od Suda poništenje dviju navedenih odluka tvrdeći, među ostalim, da je odluka o odgovarajućoj razini zaštite podataka donesena prekoračenjem ovlasti, da članak 95. UEZ-a (koji je postao članak 114. UFEU-a) nije primjerena pravna osnova za odluku kojom se odobrava sklapanje sporazuma te da su u obama slučajevima povrijeđena temeljna prava.

Što se tiče odluke o odgovarajućoj razini zaštite podataka, Sud ponajprije razmatra je li Komisija mogla valjano donijeti svoju odluku na temelju Direktive 95/46. U vezi s time Sud utvrđuje da je iz odluke o odgovarajućoj razini zaštite podataka proizlazilo da je prijenos podataka iz PNR-a CBP-u predstavljao obradu čiji su predmet bili javna sigurnost i kaznenopravne aktivnosti države. Sud je smatrao da – iako su podatke iz PNR-a početno prikupljali zračni prijevoznici u okviru djelatnosti koja je obuhvaćena pravom Unije, odnosno prodaje zrakoplovnih karata koje su davale pravo na pružanje

[28] Odluka Komisije 2004/535/EZ od 14. svibnja 2004. o utvrđivanju odgovarajuće razine zaštite osobnih podataka sadržanih u evidenciji podataka o putnicima prenesenih Uredu za carinsku i graničnu zaštitu SAD-a (SL 2004., L 235, str. 11.)

[29] Odluka Vijeća 2004/496/EZ od 17. svibnja 2004. o sklapanju Sporazuma između Europske zajednice i Sjedinjenih Američkih Država o obradi i prijenosu podataka iz evidencije podataka o putnicima (PNR) zračnih prijevoznika Ministarstvu za domovinsku sigurnost Sjedinjenih Američkih Država, Uredu za carinsku i graničnu zaštitu (SL 2004., L 183, str. 83.)

usluga – obrada podataka o kojoj je bila riječ u odluci o odgovarajućoj razini zaštite podataka bila je posve druge naravi. Naime, ta se odluka nije odnosila na obradu podataka potrebnu za pružanje usluga, nego na obradu podataka koja se smatrala potrebnom za očuvanje javne sigurnosti i u represivne svrhe.

U tom pogledu Sud navodi da činjenica da su privatni operatori prikupljali podatke iz PNR-a u komercijalne svrhe te organizirali njihov prijenos u treće države nije sprečavala to da se taj prijenos smatra obradom podataka koja je isključena iz područja primjene Direktive. Naime, ta je obrada bila dio okvira koji su uspostavile javne vlasti radi javne sigurnosti. Posljedično, Sud zaključuje da odluka o odgovarajućoj razini zaštite podataka nije ulazila u područje primjene Direktive jer se odnosila na obradu osobnih podataka koja je iz nje isključena. Stoga Sud poništava odluku o odgovarajućoj razini zaštite podataka.

U odnosu na odluku Vijeća, Sud utvrđuje da se na članku 95. UEZ-a u vezi s člankom 25. Direktive 95/46 ne može temeljiti nadležnost Zajednice za sklapanje predmetnog sporazuma s SAD-om. Naime, taj se sporazum odnosio na isti prijenos podataka kao i odluka o odgovarajućoj razini zaštite podataka i stoga na obrade podataka koje su bile isključene iz područja primjene Direktive. Stoga je Sud poništio odluku Vijeća o odobravanju sklapanja Sporazuma.

Presuda od 13. svibnja 2014. (veliko vijeće), Google Spain i Google (C-131/12, EU:C:2014:317)

Španjolski državljanin podnio je 2010. Agenciji Española de Protección de Datos (Španjolska agencija za zaštitu podataka, u daljnjem tekstu: AEPD) prigovor protiv La Vanguardia Edicionesa SL, izdavača visokotiražnih dnevnih novina u Španjolskoj, kao i protiv Googlea Spain i Googlea Inc. On je tvrdio da su se internetskim korisnicima prilikom unošenja njegova imena u internetski pretraživač grupe Google prikazivali rezultati s poveznicama prema dvjema stranicama dnevnika La Vanguardia iz 1998. na kojima se, među ostalim, nalazio oglas za prodaju nekretnina na dražbi u postupku ovrhe radi naplate njegovih dugova. On je tim prigovorom zatražio, s jedne strane, da se La Vanguardiji naloži brisanje ili izmjena predmetnih stranica odnosno primjena određenih alata internetskih pretraživača radi zaštite tih podataka. S druge je strane zatražio da se društvu Google Spain ili Google Inc. naloži brisanje ili prikrivanje njegovih osobnih podataka kako se oni više ne bi pojavljivati u rezultatima pretrage i poveznicama La Vanguardije.

AEPD je odbio prigovor protiv La Vanguardije, ocjenjujući da je urednik zakonito objavio informacije o kojima je riječ, ali ga je, nasuprot tomu, prihvatio u dijelu u kojem je bio usmjeren protiv društava Google Spain i Google Inc. te je od njih zatražio da poduzmu potrebne mjere kako bi se iz njihovih indeksa uklonili podaci i kako bi im ubuduće bio onemogućen pristup. Navedena društva uložila su pred Audiencijom Nacional (Visoki nacionalni sud, Španjolska) dvije žalbe radi poništenja AEPD-ove odluke, a nacionalni sud uputio je niz pitanja Sudu.

Sud je u toj presudi također odlučivao o teritorijalnom području primjene Direktive 95/46.

Sud tako presuđuje da je obrada osobnih podataka izvršena u okviru aktivnosti poslovnog nastana voditelja obrade na državnom području države članice u smislu Direktive 95/46 kad operator pretraživača, iako ima svoje sjedište u trećoj državi, osnuje u državi članici podružnicu ili društvo kćer u cilju promocije i prodaje oglašivačkih prostora na pretraživaču i čija je aktivnost usmjerena na stanovnike te države članice.

Naime, u tim okolnostima aktivnosti operatora pretraživača i njegova poslovnog nastana smještenog u državi članici, iako su različite, neodvojivo su povezane, s obzirom na to da aktivnosti povezane s oglašivačkim prostorima predstavljaju način na koji je pretraživač o kojem je riječ ekonomski isplativ i s obzirom na to da je taj pretraživač istodobno sredstvo koje omogućuje ostvarenje tih aktivnosti.

Presuda od 11. prosinca 2014., Ryneš (C-212/13, EU:C:2014:2428)

Kao odgovor na ponovljene napade F. Ryneš postavio je na svoju kuću nadzornu kameru. Nakon novog napada na njegovu kuću snimke navedene kamere omogućile su identifikaciju dvaju osumnjičenika protiv kojih je pokrenut kazneni postupak. Jedan od osumnjičenika osporavao je pred češkim Uredom za zaštitu osobnih podataka zakonitost obrade podataka snimljenih nadzornom kamerom, nakon čega je taj ured utvrdio da je F. Ryneš povrijedio pravila u području zaštite osobnih podataka te mu je izrekao novčanu kaznu.

Postupajući povodom kasacijske žalbe F. Ryneša protiv odluke Městský soud v Praze (Gradski sud u Pragu, Češka Republika) kojom je potvrđena odluka Ureda, Nejvyšší správní soud (Visoki upravni sud) postavio je Sudu upit predstavlja li Rynešovo snimanje u cilju zaštite njegova života, zdravlja i imovine obradu podataka koja nije obuhvaćena Direktivom 95/46 jer to snimanje provodi fizička osoba tijekom aktivnosti isključivo osobne ili domaće naravi u smislu članka 3. stavka 2. druge alineje navedene direktive.

Sud presuđuje da uporaba sustava kamere, zahvaljujući kojem je snimljen videozapis osoba koji je pohranjen na uređaj za kontinuirano snimanje kao što je to tvrdi disk, koji je fizička osoba postavila na svoju obiteljsku kuću u cilju zaštite imovine, zdravlja i života vlasnika kuće, pri čemu taj sustav nadzire i javni prostor, ne predstavlja obradu podataka koja se provodi za obavljanje isključivo osobnih ili domaćih aktivnosti.

U tom pogledu Sud podsjeća na to da zaštita temeljnog prava na privatnost, zajamčena člankom 7. Povelje, zahtijeva da su odstupanja i ograničenja u zaštiti osobnih podataka u granicama onoga što je krajnje nužno. Budući da se odredbe Direktive 95/46, uređujući obradu osobnih podataka koja može povrijediti temeljne slobode i, među ostalim, pravo na privatnost, nužno moraju tumačiti s obzirom na temeljna prava koja su sadržana u Povelji, odstupanje predviđeno člankom 3. stavkom 2. drugom alinejom mora se usko tumačiti. Usto, iz samog teksta te odredbe proizlazi da se Direktiva 95/46 ne primjenjuje na obradu podataka koja se provodi tijekom aktivnosti „isključivo” osobne ili domaće

naravi. Međutim, ako videonadzor obuhvaća, makar i djelomično, javni prostor te je zbog te činjenice usmjeren prema vanjskom dijelu privatnog područja osobe koja na taj način provodi obradu podataka, ta se obrada ne može smatrati isključivo „osobnom ili domaćom" aktivnošću u smislu navedene odredbe.

Presuda od 16. siječnja 2024. (veliko vijeće), Österreichische Datenschutzbehörde (C-33/22, EU:C:2024:46)

Kako bi se ispitao mogući politički utjecaj na Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (Savezni ured za zaštitu Ustava i borbu protiv terorizma, Austrija)[30], Nationalrat (Nacionalno vijeće, Austrija) osnovao je istražno povjerenstvo (u daljnjem tekstu: istražno povjerenstvo za BVT). To je povjerenstvo saslušalo osobu WK kao svjedoka. Unatoč njegovu zahtjevu za anonimizaciju, u zapisniku s tog saslušanja, objavljenom na internetskoj stranici Parlamenta Österreich (Parlament Austrije), bilo je navedeno puno ime i prezime tog svjedoka. Tvrdeći da je takvo otkrivanje njezina identiteta protivno OUZP-u i austrijskom zakonodavstvu, osoba WK podnijela je pritužbu Österreichische Datenschutzbehördeu (Tijelo za zaštitu podataka, Austrija, u daljnjem tekstu: Datenschutzbehörde). Odlukom od 18. rujna 2019. Datenschutzbehörde proglasio se nenadležnim za odlučivanje o pritužbi, pri čemu je objasnio da načelo diobe vlasti isključuje mogućnost da on, kao tijelo izvršne vlasti, provodi nadzor nad istražnim povjerenstvom za BVT, koje je dio zakonodavne vlasti.

Nakon odluke Bundesverwaltungsgerichta (Savezni upravni sud, Austrija), koji je prihvatio tužbu osobe WK i poništio odluku Datenschutzbehördea, potonji je protiv odluke Saveznog upravnog suda podnio reviziju Visokom upravnom sudu.

U tom je kontekstu sud koji je uputio zahtjev pitao Sud jesu li aktivnosti istražnog povjerenstva koje je osnovao parlament države članice obuhvaćene područjem primjene OUZP-a i primjenjuje li se ta uredba kada se te aktivnosti odnose na zaštitu nacionalne sigurnosti.

Kao prvo, Sud podsjeća na to da je jedini cilj članka 2. stavka 2. točke (a) OUZP-a, kojim se propisuje da se ta uredba ne primjenjuje na obradu osobnih podataka tijekom djelatnosti koja nije obuhvaćena opsegom prava Unije, isključiti iz područja primjene te uredbe obrade koje državna tijela provode u okviru aktivnosti namijenjene zaštiti nacionalne sigurnosti ili neke druge aktivnosti koja se može svrstati u istu kategoriju. Na taj način sama činjenica da je neka aktivnost specifična za državu ili tijelo javne vlasti nije dovoljna da se automatski isključi primjena OUZP-a na takvu aktivnost.

To tumačenje, koje proizlazi iz nepostojanja razlikovanja s obzirom na identitet voditelja obrade o kojem je riječ, potvrđeno je člankom 4. točkom 7. OUZP-a[31].

[30] To je tijelo 1. prosinca 2021. postalo „Direktion Staatsschutz und Nachrichtendienst" (Uprava za državnu sigurnost i obavještajnu službu, Austrija).

[31] Njime se pojam „voditelj obrade" definira na način da znači „fizičk[u] ili pravn[u] osob[u], tijelo javne vlasti, agencij[u] ili drugo tijelo koje samo ili zajedno s drugima određuje svrhe i sredstva obrade".

Sud pojašnjava da parlamentarna priroda istražnog povjerenstva za BVT ne znači da su aktivnosti tog povjerenstva isključene iz područja primjene OUZP-a. Naime, iznimka predviđena u članku 2. stavku 2. točki (a) OUZP-a upućuje samo na kategorije aktivnosti koje zbog svoje prirode nisu obuhvaćene područjem primjene prava Unije, a ne na kategorije osoba. Prema tome, na temelju okolnosti kao takve, da obradu osobnih podataka provodi istražno povjerenstvo koje je osnovao parlament države članice izvršavajući svoju nadzornu ovlast izvršne vlasti, ne može se utvrditi da se ta obrada provodi tijekom djelatnosti koja nije obuhvaćena opsegom prava Unije.

Kao drugo, Sud ističe da, iako je na državama članicama da definiraju svoje osnovne sigurnosne interese i donesu prikladne mjere za njihovo osiguranje[32], sama činjenica da je nacionalna mjera donesena radi zaštite nacionalne sigurnosti ne može dovesti do neprimjenjivosti prava Unije i osloboditi države članice od nužnog poštovanja tog prava. Naime, iznimka predviđena u članku 2. stavku 2. točki (a) OUZP-a upućuje samo na kategorije aktivnosti koje zbog svoje prirode nisu obuhvaćene područjem primjene prava Unije. U tom pogledu, okolnost da je voditelj obrade javno tijelo čija je glavna aktivnost osiguranje nacionalne sigurnosti nije sama po sebi dovoljna da bi se iz područja primjene OUZP-a isključile obrade osobnih podataka koje to tijelo provodi u okviru drugih aktivnosti koje obavlja.

U ovom se slučaju ne čini da politički nadzor koji provodi istražno povjerenstvo za BVT predstavlja, kao takav, aktivnost namijenjenu zaštiti nacionalne sigurnosti ili neku drugu aktivnost koja se može svrstati u istu kategoriju. Stoga, pod uvjetom da to provjeri sud koji je uputio zahtjev, ta aktivnost nije izvan područja primjene OUZP-a.

S obzirom na navedeno, parlamentarno istražno povjerenstvo može imati pristup osobnim podacima koji, zbog razloga koji se odnose na nacionalnu sigurnost, moraju uživati posebnu zaštitu. U tom se pogledu zakonodavnim mjerama mogu utvrditi ograničenja obveza i prava iz OUZP-a kako bi se zajamčila, među ostalim, nacionalna sigurnost[33]. Tako se na tom temelju mogu opravdati ograničenja u odnosu na prikupljanje osobnih podataka, obavještavanje ispitanika i njihov pristup navedenim podacima ili pak njihovo otkrivanje, bez privole ispitanika, osobama koje nisu voditelj obrade, pod uvjetom da se takvim ograničenjima poštuje bit temeljnih prava i sloboda ispitanika te da predstavljaju nužnu i proporcionalnu mjeru u demokratskom društvu.

Međutim, Sud napominje da iz informacija koje su mu stavljene na raspolaganje ne proizlazi da je istražno povjerenstvo za BVT tvrdilo da je otkrivanje osobnih podataka ispitanika bilo nužno za zaštitu nacionalne sigurnosti i utemeljeno na nacionalnoj zakonodavnoj mjeri predviđenoj u tu svrhu, što je na sudu koji je uputio zahtjev da provjeri po potrebi.

[32] U skladu s člankom 4. stavkom 2. UEU-a

[33] U skladu s člankom 23. OUZP-a

2. Pojam „osobni podaci”

Presuda od 19. listopada 2016., Breyer (C-582/14, EU:C:2016:779)

P. Breyer podnio je pred njemačkim građanskim sudovima tužbu kojom je zatražio da se Saveznoj Republici Njemačkoj zabrani pohranjivanje i povjeravanje trećim osobama na pohranjivanje informatičkih podataka koji su se prenosili nakon svakog posjeta internetskim stranicama njemačkih saveznih službi. Naime, kako bi spriječio napade i omogućio kazneni progon napadača, pružatelj usluga internetskih medija njemačkih saveznih službi registrirao je podatke o „dinamičnoj” adresi IP-a, tj. adresi koja se mijenja prilikom svakog novog povezivanja na internet, te o datumu i vremenu sesije posjeta stranici. Za razliku od statičnih adresa IP-a, dinamične adrese IP-a ne omogućuju a priori povezivanje, preko datoteka dostupnih javnosti, određenog računala i fizičkog mrežnog priključka kojim se koristi pružatelj internetskog pristupa. Sami pohranjeni podaci ne omogućuju pružatelju usluga internetskih medija identifikaciju korisnika. Nasuprot tomu, pružatelj internetskog pristupa raspolaže dodatnim informacijama koje, ako se povežu s tom adresom IP-a, omogućuju identifikaciju tog korisnika.

U tom je kontekstu Bundesgerichtshof (Savezni vrhovni sud, Njemačka), postupajući u revizijskom postupku, postavio Sudu upit predstavlja li za pružatelja usluga informatičkih medija adresa IP-a koju on pohrani prilikom posjeta osobe njegovoj internetskoj stranici osobni podatak.

Sud prije svega navodi da, kako bi podatak bio „osobni podatak” u smislu članka 2. točke (a) Direktive 95/46, nije nužno da se sve informacije potrebne za identifikaciju dotične osobe nalaze u posjedu samo jedne osobe. Činjenica da dodatne informacije potrebne za identifikaciju korisnika internetske stranice ne posjeduje pružatelj usluga internetskih medija, nego pružatelj internetskog pristupa tog korisnika, nije stoga takva da isključuje da su dinamične adrese IP-a koje pohranjuje pružatelj usluga internetskih medija za njega osobni podaci u smislu članka 2. točke (a) Direktive 95/46.

Posljedično, Sud utvrđuje da dinamična adresa IP-a koju pohrani pružatelj usluga informatičkih medija prilikom posjeta osobe internetskoj stranici koju taj pružatelj čini dostupnom javnosti u odnosu na tog pružatelja predstavlja osobni podatak u smislu članka 2. točke (a) Direktive 95/46, ako raspolaže pravnim sredstvima koja mu omogućuju identifikaciju navedene osobe pomoću dodatnih informacija kojima raspolaže pružatelj internetskog pristupa te osobe.

Presuda od 20. prosinca 2017., Nowak (C-434/16, EU:C:2017:994)

P. Nowak, računovođa na osposobljavanju, nije uspio položiti ispit koji je organizirala irska strukovna organizacija računovođa. Na temelju članka 4. Zakona o zaštiti podataka on je podnio zahtjev za pristup koji se odnosio na sve njegove osobne podatke koje je u posjedu imala strukovna organizacija računovođa. Ta je strukovna organizacija P.

Nowaku dostavila određene dokumente, ali mu je odbila proslijediti presliku ispitnog rada uz obrazloženje da on nije sadržavao osobne podatke koji se na njega odnose u smislu Zakona o zaštiti podataka.

Budući da iz istih tih razloga službenik za zaštitu podataka nije udovoljio zahtjevu P. Nowaka za pristup, potonji se obratio nacionalnim sudovima. Supreme Court (Vrhovni sud, Irska), postupajući povodom žalbe P. Nowaka, postavio je Sudu upit treba li članak 2. točku (a) Direktive 95/46 tumačiti na način da su u okolnostima poput onih u glavnom postupku pisani odgovori kandidata tijekom stručnog ispita i eventualne povezane napomene ispitivača u vezi s tim odgovorima osobni podaci kandidata u smislu te odredbe.

Kao prvo, Sud navodi da, kako bi podatak bio „osobni podatak” u smislu članka 2. točke (a) Direktive 95/46, nije nužno da se sve informacije potrebne za identifikaciju dotične osobe nalaze u posjedu samo jedne osobe. Osim toga, nije sporno da, u slučaju da ispitivač ne poznaje identitet kandidata prilikom ocjenjivanja odgovora koje je on dao na ispitu, tijelo koje organizira ispit, u ovom slučaju strukovna organizacija, naprotiv, raspolaže potrebnim informacijama za identifikaciju bez poteškoća ili dvojbi tog kandidata pomoću njegova identifikacijskog broja, koji se nalazi na ispitnom radu ili njegovoj naslovnici, i tako mu može pripisati njegove odgovore.

Kao drugo, Sud utvrđuje da su pisani odgovori kandidata na stručnom ispitu podaci povezani s tom osobom. Naime, sadržaj tih odgovora odražava razinu znanja i sposobnosti kandidata u određenom području i, prema potrebi, njegov misaoni proces, rasuđivanje i kritički duh. Usto, prikupljanje takvih odgovora ima za cilj ocijeniti profesionalne kapacitete kandidata i njegovu sposobnost za obavljanje dotične struke. Štoviše, uporaba tih podataka, koja rezultira uspjehom ili neuspjehom kandidata na dotičnom ispitu, može imati učinak na njegova prava i interese jer može odrediti ili utjecati, primjerice, na njegove prilike pristupanja željenom zanimanju ili poslu. Utvrđenje da su pisani odgovori kandidata na stručnom ispitu podaci koji se odnose na tog kandidata zbog svojeg sadržaja, cilja i učinka usto također vrijedi kad je riječ o *open book* ispitu.

Kao treće, što se tiče napomena ispitivača uz odgovore kandidata, Sud smatra da su one, kao i odgovori kandidata na ispitu, podaci koji se odnose na tog kandidata jer odražavaju mišljenje ili ocjenu ispitivača o pojedinačnom uspjehu kandidata na ispitu, a osobito o njegovim znanjima i sposobnostima u dotičnom području. Osim toga, upravo je cilj navedenih napomena dokumentirati ispitivačevu ocjenu uspjeha kandidata i mogu imati učinke za potonjeg.

Kao četvrto, Sud smatra da pisani odgovori kandidata na stručnom ispitu i eventualne povezane napomene ispitivača mogu biti podvrgnuti provjeri, među ostalim, njihove točnosti i nužnosti njihova čuvanja u smislu članka 6. stavka 1. točaka (d) i (e) Direktive 95/46 i mogu biti predmet ispravka ili brisanja na temelju njezina članka 12. točke (b).

Davanje kandidatu prava na pristup tim odgovorima i tim napomenama na temelju članka 12. točke (a) te direktive služi njezinu cilju jamstva zaštite prava na privatnost tog kandidata u pogledu obrade podataka koji se na njega odnose, i to neovisno o tome ima li taj kandidat takvo pravo na pristup također na temelju nacionalnih propisa primjenjivih na ispitni postupak. Međutim, Sud naglašava da prava na pristup i ispravak na temelju članka 12. točaka (a) i (b) Direktive 95/46 ne obuhvaćaju ispitna pitanja, koja kao takva nisu osobni podaci kandidata.

S obzirom na ta razmatranja, Sud zaključuje da su u okolnostima poput onih u glavnom postupku pisani odgovori kandidata na stručnom ispitu i eventualne napomene ispitivača u vezi s tim odgovorima osobni podaci u smislu članka 2. točke (a) Direktive 95/46.

3. Pojam „obrada osobnih podataka”

Presuda od 6. studenoga 2003. (veliko vijeće), Lindqvist (C-101/01, EU:C:2003:596)

B. Lindqvist, volonterka u župi protestantske crkve u Švedskoj, izradila je na svojem osobnom računalu internetske stranice na kojima je objavila osobne podatke o većem broju osoba koje su, kao i ona, volontirale u okviru navedene župe. B. Lindqvist osuđena je na plaćanje novčane kazne jer je uporabila osobne podatke u okviru automatske obrade, pri čemu nije prethodno podnijela pisanu izjavu švedskom Datainspektionu (javno tijelo za zaštitu računalno prenesenih podataka), jer je te podatke bez odobrenja prenijela trećim zemljama i jer je obrađivala osjetljive osobne podatke.

U okviru žalbe B. Lindqvist protiv te odluke pred Göta hovrättom (Žalbeni sud, Švedska) taj je sud postavio prethodno pitanje Sudu je li B. Lindqvist „u cijelosti ili djelomično [obrađivala osobne podatke] automatskim putem” u smislu Direktive 95/46.

Sud utvrđuje da upućivanje na različite osobe na internetskoj stranici i njihovo identificiranje imenom ili na drugi način, primjerice navođenjem njihova telefonskog broja ili informacija u vezi s njihovim radnim uvjetima ili hobijima, predstavlja „u cijelosti ili djelomično [obrađivanje osobnih podataka] automatskim putem” u smislu te direktive. Naime, takva obrada osobnih podataka koja se provodi radi obavljanja volonterskih ili vjerskih aktivnosti nije obuhvaćena nijednom iznimkom od područja primjene Direktive jer ne ulazi ni u kategoriju aktivnosti koje se odnose na javnu sigurnost ni u kategoriju aktivnosti isključivo osobne ili domaće naravi koje su izvan područja primjene Direktive.

Presuda od 13. svibnja 2014. (veliko vijeće), Google Spain i Google (C-131/12, EU:C:2014:317)

U toj presudi (vidjeti također poglavlje II.1., naslovljeno „Područje primjene općih propisa”) Sud je imao priliku pojasniti pojam „obrada osobnih podataka” na internetu u pogledu Direktive 95/46.

Sud je tako presudio da aktivnost pretraživača koja se sastoji u pronalaženju informacija koje su treće strane objavile ili stavile na internet, njihovom automatskom indeksiranju, privremenom pohranjivanju i, naposljetku, stavljanju na raspolaganje internetskim korisnicima u redoslijedu prema zadanim postavkama treba kvalificirati kao obradu osobnih podataka ako te informacije sadržavaju osobne podatke. Usto, Sud podsjeća na to da operacije koje se navode u Direktivi treba kvalificirati kao obradu i u slučaju kad se odnose isključivo na informacije koje su već objavljene u medijima. Opće odstupanje od primjene Direktive u takvom bi joj slučaju uvelike oduzelo smisao.

Presuda od 10. srpnja 2018. (veliko vijeće), Jehovan todistajat (C-25/17, EU:C:2018:551)

Finsko tijelo za zaštitu podataka donijelo je odluku kojom se zajednici Jehovinih svjedoka zabranjuje prikupljanje ili obrada osobnih podataka u okviru aktivnosti propovijedanja njezinih članova od vrata do vrata ako se pritom ne poštuju uvjeti iz finskog zakonodavstva u vezi s obradom takvih podataka. Naime, članovi te zajednice u okviru svoje aktivnosti propovijedanja od vrata do vrata vode bilješke o posjetima osobama koje oni sami ili navedena zajednica ne poznaju. Ti se podaci prikupljaju kao podsjetnik, kako bi se mogli pronaći prilikom mogućeg kasnijeg posjeta, pri čemu dotične osobe na to nisu pristale niti su o tome obaviještene. U tom pogledu zajednica Jehovinih svjedoka dala je svojim članovima smjernice o vođenju takvih bilješki, koje su bile objavljene u barem jednoj od njezinih publikacija posvećenih aktivnosti propovijedanja.

Sud presuđuje da prikupljanje osobnih podataka koje provode članovi vjerske zajednice u okviru aktivnosti propovijedanja od vrata do vrata i naknadne obrade tih podataka nisu obuhvaćeni iznimkama od područja primjene Direktive 95/46, s obzirom na to da ne predstavljaju ni obrade osobnih podataka tijekom aktivnosti iz članka 3. stavka 2. prve alineje te direktive ni obrade osobnih podataka koje provode fizičke osobe tijekom aktivnosti isključivo osobne ili domaće naravi u smislu članka 3. stavka 2. druge alineje navedene direktive.

Presuda od 22. lipnja 2021. (veliko vijeće), Latvijas Republikas Saeima (Kazneni bodovi) (C-439/19, EU:C:2021:504)

B je fizička osoba kojoj su izrečeni kazneni bodovi zbog jednog ili više prometnih prekršaja. Ceļu satiksmes drošības direkcija (Uprava za sigurnost cestovnog prometa, Latvija, u daljnjem tekstu: CSDD) te je kaznene bodove upisala u Nacionalni registar vozila i njihovih vozača.

Na temelju latvijskog propisa o cestovnom prometu[34] informacije o kaznenim bodovima izrečenima vozačima vozila upisanih u taj registar javno su dostupne te ih CSDD

[34] Članak 141 stavak 2. Ceļu satiksmes likumsa (Zakon o cestovnom prometu) od 1. listopada 1997. (Latvijas Vēstnesis, 1997., br. 274/276)

priopćava svakoj osobi koja to zatraži – uključujući i gospodarskim subjektima radi ponovne uporabe – pri čemu nije potrebno opravdati poseban interes za dobivanje tih podataka. Dvojeći o zakonitosti tog propisa, osoba B podnijela je ustavnu tužbu Latvijas Republikas Satversmes tiesi (Ustavni sud, Latvija) kako bi se ispitala usklađenosti tog propisa s pravom na poštovanje privatnosti.

Ustavni sud smatrao je da u okviru ocjene tog ustavnog prava mora voditi računa o OUZP-u. Stoga je od Suda zatražio da pojasni doseg više odredbi OUZP-a kako bi mogao utvrditi je li latvijski propis o cestovnom prometu u skladu s tom uredbom.

U svojoj presudi, donesenoj u velikom vijeću, Sud ocjenjuje da obrada osobnih podataka o kaznenim bodovima jest „obrada osobnih podataka koji se odnose na kaznene osude i kažnjiva djela”[35], za koju OUZP predviđa pojačanu zaštitu zbog posebne osjetljivosti odnosnih podataka.

S tim u vezi on uvodno napominje da su informacije o kaznenim bodovima osobni podaci i da CSDD-ovo priopćavanje tih informacija trećim osobama čini obradu koja je obuhvaćena materijalnim područjem primjene OUZP-a. Naime, to područje primjene vrlo je široko, a spomenuta obrada nije obuhvaćena iznimkama od primjene te uredbe.

Tako, s jedne strane, navedena obrada nije obuhvaćena iznimkom o neprimjeni OUZP-a na obradu izvršenu tijekom djelatnosti koja nije obuhvaćena opsegom prava Unije[36]. Treba smatrati da je jedini cilj te iznimke isključivanje iz područja primjene te uredbe obrada osobnih podataka koje državna tijela provode u okviru aktivnosti namijenjenih zaštiti nacionalne sigurnosti ili neke druge aktivnosti koja se može svrstati u istu kategoriju. Te aktivnosti konkretno obuhvaćaju one kojima je cilj zaštita osnovnih državnih funkcija i temeljnih interesa društva. Međutim, aktivnosti vezane uz sigurnost cestovnog prometa nemaju takav cilj te se stoga ne mogu svrstati u kategoriju aktivnosti kojima je cilj zaštita nacionalne sigurnosti.

S druge strane, priopćavanje osobnih podataka o kaznenim bodovima nije ni obrada obuhvaćena iznimkom o neprimjeni OUZP-a na obrade osobnih podataka koje nadležna tijela obavljaju u kaznenim stvarima[37]. Naime, Sud ocjenjuje da se prilikom navedenog priopćavanja CSDD ne može smatrati takvim „nadležnim tijelom”[38].

35 Članak 10. OUZP-a

36 Članak 2. stavak 2. točka (a) OUZP-a

37 Članak 2. stavak 2. točka (d) OUZP-a

38 Članak 3. stavak 7. Direktive (EU) 2016/680 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka od strane nadležnih tijela u svrhe sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Okvirne odluke Vijeća 2008/977/PUP (SL 2016., L 119, str. 89. i ispravak SL 2018., L 127, str. 14.)

Kako bi utvrdio čini li pristup osobnim podacima o prometnim prekršajima, poput kaznenih bodova, obradu osobnih podataka koji se odnose na „kažnjiva djela”[39] te uživaju pojačanu zaštitu, Sud zaključuje, oslanjajući se osobito na okolnosti nastanka OUZP-a, da taj pojam upućuje isključivo na kaznena djela. Međutim, činjenica da se u latvijskom pravnom sustavu prometni prekršaji kvalificiraju kao prekršajni nije odlučna za ocjenu jesu li ta kažnjiva djela obuhvaćena pojmom „kazneno djelo” s obzirom na to da je riječ o autonomnom pojmu prava Unije koji zahtijeva autonomno i ujednačeno tumačenje u cijeloj Uniji. Na taj način, nakon što je podsjetio na tri kriterija relevantna za ocjenu kaznene naravi kažnjivog djela – a to su pravna kvalifikacija kažnjivog dijela u nacionalnom pravu, narav kažnjivog djela i težina izrečene kazne – Sud ocjenjuje da su prometni prekršaji o kojima je riječ obuhvaćeni pojmom „kažnjiva djela” u smislu OUZP-a. Kad je riječ o prvim dvama kriterijima, Sud navodi da, čak i ako se kažnjiva djela u nacionalnom pravu ne kvalificiraju kao „kaznena”, to može proizlaziti iz njihove naravi, a osobito iz represivne svrhe sankcije do čijeg izricanja može doći. U predmetnom slučaju, izricanje kaznenih bodova za prometne prekršaje, baš kao i druge sankcije do kojih može dovesti njihovo počinjenje, služe, među ostalim, navedenoj represivnoj svrsi. Kad je riječ o trećem kriteriju, Sud napominje da samo prometni prekršaji određene težine dovode do izricanja kaznenih bodova i da, samim time, mogu dovesti do kazni određene težine. Nadalje, izricanje kaznenih bodova u pravilu prati sankcija koja se izriče, a kumuliranje tih bodova dovodi do pravnih posljedica koje mogu uključivati čak i zabranu upravljanja vozilom.

Presuda od 5. prosinca 2023. (veliko vijeće), Nacionalinis visuomenės sveikatos centras (C-683/21, EU:C:2023:949)

Kako bi bolje upravljala pandemijom bolesti COVID-19, litavska su tijela 2020. odlučila organizirati nabavu mobilne informatičke aplikacije. Ta je aplikacija trebala pridonijeti epidemiološkom praćenju tako što omogućuje bilježenje i praćenje podataka o osobama koje su bile izložene virusu bolesti COVID-19.

U tu je svrhu Nacionalinis visuomenės sveikatos centras prie Sveikatos apsaugos ministerijos (Nacionalni centar za javno zdravstvo pri Ministarstvu zdravstva, Litva, u daljnjem tekstu: NVSC), zadužen za tu nabavu, kontaktirao društvo UAB „IT sprendimai sėkmei” (u daljnjem tekstu: ITSS), zahtijevajući od njega da razvije takvu mobilnu aplikaciju. Nakon toga zaposlenici NVSC-a uputili su tom društvu poruke elektroničke pošte koje se osobito odnose na pitanja koja će se postavljati u toj aplikaciji.

U razdoblju od travnja do svibnja 2020. mobilna aplikacija koju je razvilo društvo ITSS bila je stavljena na raspolaganje javnosti. Slijedom toga, 3802 osobe koristile su se tom aplikacijom i dostavile različite podatke koji se na njih odnose, a koje je navedena

[39] Članak 10. OUZP-a

aplikacija tražila. Međutim, zbog nedostatka financijskih sredstava NVSC nije dodijelio društvu ITSS nikakav ugovor o javnoj nabavi s ciljem službene nabave njegove mobilne aplikacije te je okončao postupak koji se na nju odnosi.

U međuvremenu je nacionalno nadzorno tijelo pokrenulo istragu u vezi s obradom osobnih podataka koja proizlazi iz upotrebe te aplikacije. Odlukom tog tijela, donesenom nakon istrage, NVSC-u i društvu ITSS, koji se smatraju zajedničkim voditeljima obrade, izrečene su upravne novčane kazne.

NVSC je osporavao tu odluku pred Vilniaus apygardos administracinis teismasom (Okružni upravni sud u Vilniusu, Litva). Budući da je dvojio o tumačenju nekoliko odredbi OUZP-a, taj je sud uputio Sudu zahtjev za prethodnu odluku.

Sud, zasjedajući u velikom vijeću, u svojoj presudi pojašnjava, među ostalim, pojam „obrada”. Sud je u tom pogledu naveo da uporaba osobnih podataka u svrhu informatičkog testiranja mobilne aplikacije čini obradu u smislu OUZP-a. Međutim, isto ne vrijedi ako su takvi podaci anonimizirani tako da se ispitanik na kojeg se ti podaci odnose ne može utvrditi ili se više ne može utvrditi ili ako se radi o fiktivnim podacima koji se ne odnose na postojeću fizičku osobu.

Naime, s jedne strane, pitanje koriste li se osobni podaci za informatička ispitivanja ili u drugu svrhu ne utječe na kvalifikaciju postupka kao „obrade”. S druge strane, samo se obrada koja se odnosi na osobne podatke može kvalificirati kao „obrada” u smislu OUZP-a. Međutim, fiktivni ili anonimizirani podaci nisu osobni podaci.

4. Pojam „sustav arhiviranja osobnih podataka”

Presuda od 10. srpnja 2018. (veliko vijeće), Jehovan todistajat (C-25/17, EU:C:2018:551)

U toj je presudi (vidjeti također poglavlje II. 3., naslovljeno „Pojam ‚obrada osobnih podataka’”) Sud pojasnio pojam „sustav arhiviranja” iz članka 2. točke (c) Direktive 95/46.

Nakon što je podsjetio na to da se ta direktiva primjenjuje na ručnu obradu osobnih podataka samo ako su obrađeni podaci sadržani ili će biti sadržani u sustavu arhiviranja, Sud tako presuđuje da navedeni pojam obuhvaća skup osobnih podataka prikupljenih u okviru aktivnosti propovijedanja od vrata do vrata koji sadržava imena i adrese te druge informacije o osobama kojima se pristupa, pod uvjetom da su ti podaci strukturirani prema određenim mjerilima koja u praksi omogućuju lakše pronalaženje radi naknadne uporabe. Kako bi taj skup bio obuhvaćen tim pojmom, nije nužno da je sastavljen od kartoteka, posebnih popisa ili drugih sustava pretraživanja.

5. Pojam „voditelj obrade osobnih podataka”

Presuda od 10. srpnja 2018. (veliko vijeće), Jehovan todistajat (C-25/17, EU:C:2018:551)

U tom je predmetu (vidjeti također poglavlja II. 3. i II. 4., naslovljena „Pojam ‚obrada osobnih podataka’” i „Pojam ‚sustav arhiviranja osobnih podataka’”) Sud odlučivao o odgovornosti vjerske zajednice u pogledu obrade osobnih podataka izvršene u okviru aktivnosti propovijedanja od vrata do vrata koju organizira, koordinira i potiče ta zajednica.

Tako Sud ocjenjuje da se ne može smatrati da obveza svake osobe da poštuje pravna pravila Unije o zaštiti osobnih podataka predstavlja zadiranje u organizacijsku autonomiju vjerskih zajednica. On u tom pogledu zaključuje da članak 2. točku (d) Direktive 95/46, u vezi s člankom 10. stavkom 1. Povelje, treba tumačiti na način da se vjerska zajednica zajedno sa svojim članovima propovjednicima može smatrati voditeljem obrada osobnih podataka koju provode navedeni članovi propovjednici u okviru aktivnosti propovijedanja od vrata do vrata koju ta zajednica organizira, koordinira i potiče a da pritom nije nužno ni da navedena zajednica ima pristup tim podacima ni da se utvrdi da je ona svojim članovima dala pisane smjernice ili savjete u vezi s tim obradama.

Presuda od 5. lipnja 2018. (veliko vijeće), Wirtschaftsakademie Schleswig Holstein (C-210/16, EU:C:2018:388)

Njemačko tijelo za zaštitu podataka naložilo je u svojstvu nadzornog tijela u smislu članka 28. Direktive 95/46 njemačkom društvu specijaliziranom u području obrazovanja, koje je nudilo usluge osposobljavanja posredstvom stranice obožavatelja koja se nalazi na internetskoj stranici društvene mreže Facebook, da deaktivira svoju stranicu obožavatelja. Naime, prema mišljenju tog tijela, ni to društvo ni Facebook nisu obavještavali posjetitelje stranice obožavatelja o tome da je potonji s pomoću kolačića prikupljao njihove osobne podatke koje su navedeno društvo i Facebook potom obrađivali.

U tom kontekstu Sud pojašnjava pojam „voditelj obrade” osobnih podataka. On u tom pogledu smatra da administrator stranice obožavatelja koja se nalazi na Facebooku, kao što je to društvo o kojem je riječ u glavnom postupku, utvrđivanjem postavki (među ostalim, s obzirom na svoju ciljanu publiku i ciljeve upravljanja svojim aktivnostima odnosno ciljeve njihove promidžbe) pridonosi utvrđivanju svrhe i načina obrade osobnih podataka posjetitelja svoje stranice obožavatelja. Stoga Sud navodi da valja smatrati da je na području Unije taj administrator suodgovoran s Facebookom Ireland (društvo kći sa sjedištem u Uniji društva Facebook sa sjedištem u SAD-u) za spomenutu obradu u smislu članka 2. točke (d) Direktive 95/46.

Presuda od 29. srpnja 2019., Fashion ID (C-40/17, EU:C:2019:629)

U tom je predmetu Sud imao priliku pojasniti pojam „voditelj obrade” u pogledu umetanja dodatka na internetsku stranicu.

U ovom je slučaju društvo Fashion ID, njemački poduzetnik koji se bavi internetskom prodajom modnih artikala, na svoju internetsku stranicu umetnulo dodatak za društvenu mrežu „Sviđa mi se” društvene mreže Facebook. Čini se da je posljedica tog umetanja to da se posjećivanjem internetske stranice društva Fashion ID posjetiteljevi osobni podaci prenose društvu Facebook Ireland. Taj se prijenos odvija a da pritom navedeni posjetitelj toga nije svjestan i neovisno o tome je li on član društvene mreže Facebook i je li kliknuo na Facebookovu tipku „Sviđa mi se”.

Verbraucherzentrale NRW, njemačka neprofitna udruga za zaštitu interesa potrošača, društvu Fashion ID prigovara da je društvu Facebook Ireland prenijelo osobne podatke posjetitelja svoje internetske stranice, s jedne strane, bez njihove privole i, s druge strane, povredom obveza obavješćivanja predviđenih odredbama koje se odnose na zaštitu osobnih podataka. Postupajući u sporu, Oberlandesgericht Düsseldorf (Visoki zemaljski sud u Düsseldorfu, Njemačka) zatražio je od Suda tumačenje nekoliko odredbi Direktive 95/46.

Sud najprije utvrđuje da se upravitelj internetske stranice, poput društva Fashion ID, može smatrati voditeljem obrade u smislu članka 2. točke (d) Direktive 95/46. Međutim, ta je odgovornost ograničena na postupak ili skup postupaka obrade osobnih podataka čiju svrhu i načine to društvo stvarno utvrđuje, odnosno na prikupljanje predmetnih podataka i njihovo otkrivanje prijenosom. Nasuprot tomu, Sud smatra da je *a priori* isključeno da društvo Fashion ID utvrđuje svrhu i načine kasnijih postupaka obrade osobnih podataka koje provodi društvo Facebook Ireland, nakon što su mu ti podaci preneseni, pa se društvo Fashion ID ne može smatrati voditeljem obrade u odnosu na te postupke u smislu tog članka 2. točke (d).

Sud usto naglašava da je nužno da i upravitelj internetske stranice i pružatelj dodatka za društvenu mrežu, kao što je to Facebook Ireland, moraju tim postupcima željeti postići zakonit interes u smislu članka 7. točke (f) Direktive 95/46, kako bi oni u tom pogledu bili opravdani.

Naposljetku, Sud pojašnjava da privolu ispitanika, predviđenu člankom 2. točkom (h) i člankom 7. točkom (a) Direktive 95/46, upravitelj internetske stranice treba dobiti jedino u odnosu na postupke obrade osobnih podataka čiju svrhu i načine stvarno utvrđuje taj upravitelj. U takvoj situaciji obveza obavješćivanja predviđena člankom 10. te direktive postoji i na strani navedenog upravitelja, pri čemu se podaci koje on mora dati ispitaniku moraju odnositi samo na postupak ili skup postupaka obrade osobnih podataka čiju svrhu i načine taj upravitelj utvrđuje.

Presuda od 5. prosinca 2023. (veliko vijeće), Nacionalinis visuomenės sveikatos centras (C-683/21, EU:C:2023:949)

U tom predmetu (vidjeti također poglavlje II.3, naslovljeno „Pojam ‚obrada osobnih podataka'") Sud ističe da se subjekt koji je od poduzetnika naručio razvoj mobilne informatičke aplikacije i koji je u tom kontekstu sudjelovao u određivanju svrha i sredstava obrade osobnih podataka koja se provodi putem te aplikacije može smatrati voditeljem obrade[40]. To razmatranje ne može dovesti u pitanje činjenica da taj subjekt nije sâm provodio postupke obrade takvih podataka, nije izričito dao svoju privolu za obavljanje konkretnih postupaka takve obrade ili za stavljanje navedene mobilne aplikacije na raspolaganje javnosti i nije nabavio tu mobilnu aplikaciju, osim ako se prije tog stavljanja na raspolaganje javnosti taj subjekt tomu izričito usprotivio kao i obradi osobnih podataka koja iz toga proizlazi.

6. Pojam „zajednički voditelj obrade"

Presuda od 5. prosinca 2023. (veliko vijeće), Nacionalinis visuomenės sveikatos centras (C-683/21, EU:C:2023:949)

U tom predmetu (vidjeti također poglavlja II.3 i II.5, naslovljena „Pojam ‚obrada osobnih podataka'" i „Pojam ‚voditelj obrade osobnih podataka'") Sud je napomenuo da kvalifikacija dvaju subjekata kao zajedničkih voditelja obrade ne pretpostavlja ni postojanje dogovora između tih subjekata o određivanju svrha i sredstava obrade osobnih podataka ni postojanje dogovora kojim se određuju uvjeti zajedničkog vođenja obrade. Točno je da na temelju OUZP-a[41] zajednički voditelji obrade međusobnim dogovorom trebaju na transparentan način odrediti svoje odgovornosti u pogledu poštovanja obveza iz te uredbe. Međutim, postojanje takvog dogovora nije preduvjet da bi se dva subjekta ili više njih kvalificiralo kao „zajednički voditelji obrade", nego obveza koja se OUZP-om nalaže zajedničkim voditeljima obrade, nakon što se kvalificiraju kao takvi, kako bi se osigurala usklađenost sa zahtjevima iz te uredbe koji se na njih odnose. Stoga ta kvalifikacija proizlazi iz same činjenice da je više subjekata sudjelovalo u određivanju svrha i sredstava obrade.

Što se tiče zajedničkog određivanja svrha i sredstava obrade predmetnih subjekata, Sud je pojasnio da njihovo sudjelovanje u tom određivanju može poprimiti različite oblike i proizlaziti i iz njihove zajedničke odluke i iz njihovih usklađenih odluka. Međutim, u potonjem slučaju te se odluke moraju nadopunjavati tako da svaka od njih ima konkretan učinak na određivanje svrha i sredstava obrade.

[40] U smislu članka 4. točke 7. OUZP-a

[41] Članak 26. stavak 1. OUZP-a, u vezi s uvodnom izjavom 79. te uredbe

7. Pretpostavke zakonitosti obrade osobnih podataka

Presuda od 16. prosinca 2008. (veliko vijeće), Huber (C-524/06, EU:C:2008:724)

Bundesamt für Migration und Flüchtlinge (Savezni ured za migracije i izbjeglice, Njemačka) vodio je središnji registar stranaca koji je objedinjavao određene osobne podatke o strancima koji borave na njemačkom državnom području u razdoblju duljem od tri mjeseca. Registar je korišten u statističke svrhe, a njime su se koristile i sigurnosne i policijske službe te pravosudna tijela u izvršavanju svojih nadležnosti u području progona i istraživanja kaznenih djela te postupanja kojima se dovodi u opasnost javna sigurnost.

H. Huber, austrijski državljanin, nastanio se u Njemačkoj 1996. kako bi ondje obavljao zanimanje neovisnog agenta za osiguranje. Smatrajući da ga se obradom njegovih podataka u predmetnom registru diskriminira, s obzirom na to da takva baza podataka ne postoji za njemačke državljane, H. Huber zatražio je uklanjanje tih podataka.

U tom je kontekstu Oberverwaltungsgericht für das Land Nordrhein-Westfalen (Visoki upravni sud Sjeverne Rajne-Vestfalije, Njemačka), postupajući u sporu, postavio Sudu upit o usklađenosti obrade osobnih podataka u predmetnom registru s pravom Unije.

Sud ponajprije podsjeća na to da pravo boravka građanina Unije na državnom području države članice koje nije državljanin nije bezuvjetno, nego može biti podložno ograničenjima. Stoga je uporaba takvog registra u cilju podrške tijelima zaduženima za primjenu propisa o pravu boravka u načelu legitimna te je, s obzirom na svoju narav, usklađena sa zabranom diskriminacije na temelju državljanstva iz članka 12. stavka 1. UEZ-a (koji je postao članak 18. prvi stavak UFEU-a). Međutim, takav registar može sadržavati samo one informacije koje su potrebne u tu svrhu u smislu Direktive o zaštiti osobnih podataka.

Kad je riječ o pojmu „potrebe” obrade u smislu članka 7. točke (e) Direktive 95/46, Sud ponajprije podsjeća na to da je riječ o autonomnom pojmu prava Unije koji se mora tumačiti na način da u potpunosti odgovara cilju Direktive 95/46, kako je definiran u njezinu članku 1. stavku 1. Sud zatim utvrđuje da je sustav obrade osobnih podataka usklađen s pravom Unije ako sadržava samo podatke koji su navedenim tijelima potrebni za primjenu tog propisa i ako njegova centraliziranost omogućava učinkovitiju primjenu tog propisa u pogledu prava boravka građana Unije koji nisu državljani te države članice.

U svakom slučaju, pohrana i obrada osobnih podataka na ime u okviru takvog registra u statističke svrhe ne mogu se smatrati potrebnima u smislu članka 7. točke (e) Direktive 95/46.

Osim toga, Sud u pogledu pitanja uporabe podataka sadržanih u registru u svrhe borbe protiv kriminaliteta navodi, među ostalim, da se taj cilj odnosi na progon počinitelja kaznenih djela, neovisno o njihovu državljanstvu. Stoga država članica ne može u

pogledu cilja borbe protiv kriminaliteta razlikovati položaj svojih državljana od položaja građana Unije koji nisu državljani te države članice, a borave na njezinu državnom području. Posljedično, različito postupanje prema tim državljanima i građanima Unije, do kojeg dolazi sustavnom obradom samo osobnih podataka građana Unije koji nisu državljani dotične države članice u cilju borbe protiv kriminaliteta, jest diskriminacija zabranjena člankom 12. stavkom 1. UEZ-a.

Presuda od 19. listopada 2016., Breyer (C-582/14, EU:C:2016:779)

Sud se u toj presudi (vidjeti također poglavlje II.2., naslovljeno „Pojam ‚osobni podaci'") očitovao o odgovoru na pitanje protivi li se članku 7. točki (f) Direktive 95/46 odredba nacionalnog prava prema kojoj pružatelj usluga internetskih medija može prikupljati i koristiti osobne podatke korisnika bez njegove dozvole samo u dijelu u kojem je to potrebno kako bi omogućio i obračunao konkretno korištenje internetskih medija dotičnog korisnika i prema kojem svrha osiguravanja općeg funkcioniranja internetskog medija ne može opravdati korištenje podataka nakon završetka sesije posjeta u tijeku.

Sud presuđuje da se predmetni propis protivi članku 7. točki (f) Direktive 95/46. Naime, na temelju te odredbe obrada osobnih podataka zakonita je ako je potrebna u svrhe zakonitog interesa koji ima voditelj obrade ili treća stranka ili stranke kojima se podaci otkrivaju, osim kada su ti podaci podređeni interesu za temeljna prava i slobode osobe čiji se podaci obrađuju. Međutim, u ovom je slučaju njemačkim propisom kategorički i općenito isključena mogućnost obrade određenih kategorija osobnih podataka, bez omogućavanja odvagivanja suprotstavljenih prava i interesa o kojima je riječ u konkretnom slučaju. Na taj je način tim propisom nezakonito ograničen doseg tog načela iz članka 7. točke (f) Direktive 95/46 jer je isključena mogućnost odvagivanja između, s jedne strane, cilja osiguranja općeg funkcioniranja internetskih medijskih stranica i, s druge strane, interesa ili temeljnih prava i sloboda korisnika.

Presuda od 27. rujna 2017., Puškár (C-73/16, EU:C:2017:725)

U glavnom postupku P. Puškár podnio je tužbu pred Najvyšším súdom Slovenskej republiky (Vrhovni sud Slovačke Republike) kojom je zahtijevao da se Finančnom riaditeľstvu (Financijsko ravnateljstvo), svima njemu podređenim poreznim uredima i Kriminálnom úradu finančnej správy (Ured za borbu protiv financijskog kriminaliteta) naloži uklanjanje njegova imena iz evidencije osoba za koje je Financijsko ravnateljstvo smatralo da su samo fiktivno obavljale upravljačke funkcije, koju je to tijelo izradilo u kontekstu naplate poreza te ju je ažuriralo zajedno s Uredom za borbu protiv financijskog kriminaliteta (u daljnjem tekstu: sporna evidencija). Usto, P. Puškár zahtijevao je i da se iz te evidencije i računalnog sustava financijske uprave ukloni svaka napomena koja se odnosi na njega.

U tim je okolnostima Najvyšší súd Slovenskej republiky (Vrhovni sud Republike Slovačke) postavio Sudu pitanje, među ostalim, mogu li se pravo na poštovanje privatnog i obiteljskog života, doma i komuniciranja, sadržano u članku 7. Povelje, te pravo na

zaštitu osobnih podataka, sadržano u njezinu članku 8., tumačiti na način da državi članici ne dopuštaju da bez privole ispitanika vodi evidencije osobnih podataka za potrebe naplate poreza, to jest da je davanje osobnih podataka na raspolaganje javnim tijelima u svrhu borbe protiv utaje poreza samo po sebi riskantno.

Sud zaključuje da se članku 7. točki (e) Direktive 95/46 ne protivi obrada osobnih podataka koju bez privole ispitanika provode tijela države članice za potrebe naplate poreza i borbe protiv utaje poreza, poput one koja je provedena izradom evidencije osoba kao što je to ona o kojoj je riječ u glavnom postupku, pod uvjetom, s jedne strane, da ta tijela na temelju nacionalnog propisa imaju zadatke koji se provode zbog javnog interesa u smislu te odredbe, da su izrada te evidencije i uvrštavanje u nju imena ispitanika zaista prikladni i nužni za ostvarivanje zadanih ciljeva te da postoje dovoljne naznake za pretpostavku da se imena ispitanika opravdano nalaze u navedenoj evidenciji i, s druge strane, da su ispunjene sve pretpostavke za zakonitost te obrade osobnih podataka koje su propisane Direktivom 95/46.

U tom pogledu Sud navodi da je na nacionalnom sudu provjera je li izrada sporne evidencije nužna za izvršavanje zadataka koji se provode zbog javnog interesa o kojima je riječ u glavnom postupku, uzimajući u obzir, među ostalim, točnu svrhu izrade sporne evidencije, pravne učinke kojima podliježu osobe koje se u njoj navode te njezinu povjerljivost. Usto, nacionalni sud dužan je provjeriti s obzirom na načelo proporcionalnosti jesu li izrada sporne evidencije i uvrštavanje u nju imena ispitanika prikladni za ostvarivanje zadanih ciljeva i postoje li manje ograničavajuća sredstva za njihovo postizanje.

Nadalje, Sud utvrđuje da uvrštavanje neke osobe u spornu evidenciju može povrijediti neka njezina prava. Naime, uvrštavanjem u tu evidenciju može se naštetiti njezinu ugledu i utjecati na njezine odnose s poreznim tijelima. Jednako tako, to uvrštavanje može utjecati na pretpostavku nedužnosti te osobe, sadržanu u članku 48. stavku 1. Povelje, kao i na slobodu poduzetništva pravnih osoba, utvrđenu člankom 16. Povelje, povezanih s fizičkim osobama koje su uvrštene u spornu evidenciju. Stoga takvo zadiranje može biti prikladno samo ako postoje dovoljne naznake za sumnju da ispitanik drži fiktivne upravljačke funkcije u pravnim osobama s kojim je povezan te time ugrožava naplatu poreza i borbu protiv utaje poreza.

Osim toga, Sud smatra da, ako bi postojali razlozi da se na temelju članka 13. Direktive 95/46 ograniče neka prava propisana njezinim člancima 6., 10., 11. i 12., poput prava ispitanika na dobivanje podataka, takvo bi ograničenje moralo biti nužno za zaštitu interesa navedenog u stavku 1. navedenog članka 13., kao što je to, među ostalim, važan gospodarski i financijski interes u poreznim pitanjima, te se temeljiti na propisima.

Presuda od 11. studenoga 2020., Orange Romania (C-61/19, EU:C:2020:901)

Orange România SA pruža usluge mobilne telekomunikacije na rumunjskom tržištu. Odlukom od 28. ožujka 2018. Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP) (Nacionalno tijelo za nadzor obrade osobnih

podataka, Rumunjska) izrekla je tom društvu novčanu kaznu jer je prikupljalo i pohranjivalo preslike osobnih isprava svojih klijenata a da oni za to nisu dali valjanu privolu.

ANSPDCP je istaknuo da je u razdoblju od 1. do 26. ožujka 2018. društvo Orange România sklapalo ugovore o pružanju usluga mobilne telekomunikacije koji su sadržavali ugovornu odredbu u kojoj je bilo navedeno da se klijenti obavještavaju o prikupljanju i pohrani preslike njihove osobne isprave te da oni za to daju svoju privolu. U polje koje se odnosilo na tu ugovornu odredbu voditelj obrade bi umetnuo kvačicu prije potpisivanja ugovora.

U tom je kontekstu Tribunalul București (Viši sud u Bukureštu, Rumunjska) zatražio od Suda da pojasni uvjete u kojima se može smatrati da je pristanak klijenata na obradu osobnih podataka valjan.

Sud ponajprije podsjeća na to da se pravom Unije[42] utvrđuje popis slučajeva u kojima se obrada osobnih podataka može smatrati zakonitom. Konkretno, privola ispitanika mora biti dobrovoljna, posebna, informirana i nedvosmislena[43]. U tom pogledu privola nije dana valjano u slučaju šutnje, unaprijed kvačicom označenog polja ili manjka aktivnosti.

Usto, ako ispitanik da privolu u vidu pisane izjave koja se odnosi i na druga pitanja, izjava mora biti dana u razumljivom i lako dostupnom obliku te uz uporabu jasnog i jednostavnog jezika. Kako bi se ispitaniku osigurala stvarna sloboda izbora, ugovorne odredbe ne smiju ispitanika dovesti u zabludu u pogledu mogućnosti da sklopi ugovor čak i ako odbije pristati na obradu svojih podataka.

Sud pojašnjava da, s obzirom na to da je društvo Orange România voditelj obrade osobnih podataka, ono mora moći dokazati zakonitost obrade tih podataka i stoga u tom slučaju postojanje valjane privole svojih klijenata. U tom pogledu, budući da se čini da dotični klijenti nisu sami označili polje koje se odnosi na prikupljanje i pohranu preslika njihovih osobnih iskaznica, na temelju same činjenice da je to polje bilo označeno ne može se utvrditi pozitivno davanje njihove privole. Na sudu koji je uputio zahtjev je da provede potrebne provjere u tom pogledu.

Sud smatra da je također na nacionalnom sudu da ocijeni osobito jesu li predmetne ugovorne odredbe mogle klijente dovesti u zabludu u pogledu mogućnosti sklapanja ugovora neovisno o odbijanju davanja privole za obradu njegovih podataka ako ne postoje pojašnjenja o tome. Sud također primjećuje da je u slučaju klijentova odbijanja davanja privole za obradu njegovih podataka, društvo Orange România tražilo da dotični klijent pisanim putem izjavi da ne pristaje ni na prikupljanje ni na pohranu preslike njegove osobne isprave. Sud smatra da takav dodatni zahtjev može neopravdano

[42] Članak 7. Direktive 95/46 i članak 6. OUZP-a
[43] Članak 2. točka (h) Direktive 95/46 i članak 4. točka 11. OUZP-a

utjecati na slobodni izbor u pogledu protivljenja tom prikupljanju i pohrani. U svakom slučaju, budući da je navedeno društvo dužno dokazati da su njegovi klijenti aktivnim postupanjem izrazili svoju privolu za obradu svojih osobnih podataka, ono ne može zahtijevati od njih da aktivno izraze svoje odbijanje.

Stoga Sud zaključuje da se ugovorom koji se odnosi na pružanje telekomunikacijskih usluga, koji sadržava ugovornu odredbu prema kojoj je ispitanik bio informiran i dao je privolu za prikupljanje i pohranu preslike svoje osobne isprave u svrhu utvrđivanja identiteta, ne može dokazati da je taj ispitanik valjano dao svoju privolu za to prikupljanje i pohranu kada je polje koje se odnosi na tu ugovornu odredbu označio voditelj obrade podataka prije potpisivanja tog ugovora, ili kada ugovorne odredbe navedenog ugovora mogu ispitanika dovesti u zabludu u pogledu mogućnosti sklapanja predmetnog ugovora čak i ako on odbije pristati na obradu svojih podataka, ili kada taj voditelj neopravdano utječe na slobodan izbor ispitanika da se protivi tom prikupljanju i pohrani, zahtijevajući od njega, kako bi odbio dati svoju privolu za te obrade, da ispuni dodatni obrazac kojim se evidentira to odbijanje.

Presuda od 22. lipnja 2021. (veliko vijeće), Latvijas Republikas Saeima (Kazneni bodovi) (C-439/19, EU:C:2021:504)

U toj presudi (vidjeti također poglavlje II.3., naslovljeno „Pojam ‚obrada osobnih podataka’”) Sud presuđuje da je OUZP-u protivan propis kojim se Ceļu satiksmes drošības direkciju (Uprava za sigurnost cestovnog prometa, Latvija, u daljnjem tekstu: CSDD) obvezuje da učini dostupnim javnosti informacije o kaznenim bodovima izrečenima vozačima vozila za prometne prekršaje, pri čemu osoba koja traži pristup ne treba opravdati poseban interes za dobivanje tih podataka. Sud utvrđuje da nije dokazana nužnost priopćavanja osobnih podataka o kaznenim bodovima izrečenima za prometne prekršaje, osobito imajući u vidu cilj poboljšanja sigurnosti cestovnog prometa, na koji se poziva latvijska vlada. Osim toga, Sud smatra da ni pravo javnog pristupa službenim dokumentima ni pravo na slobodu informiranja ne opravdavaju takav propis.

S tim u vezi Sud naglašava da poboljšanje sigurnosti cestovnog prometa, koje se nastoji ostvariti latvijskim propisom, jest cilj od općeg interesa koji priznaje Unija i da stoga države članice mogu kvalificirati sigurnost cestovnog prometa kao „zadaću od javnog interesa”[44]. Međutim, nije dokazana nužnost latvijskog sustava priopćavanja osobnih podataka o kaznenim bodovima za postizanje namjeravanog cilja. Naime, s jedne strane, latvijski zakonodavac raspolaže velikim brojem metoda koje bi mu mogle omogućiti postizanje tog cilja drugim sredstvima kojima se manje zadire u temeljna prava ispitanika. S druge strane, valja voditi računa o osjetljivosti podataka o kaznenim

[44] Na temelju članka 6. stavka 1. točke (e) OUZP-a, obrada osobnih podataka je zakonita ako je „nužna za izvršavanje zadaće od javnog interesa”.

bodovima i o činjenici da njihovo javno priopćavanje može činiti ozbiljno zadiranje u prava na poštovanje privatnosti i na zaštitu osobnih podataka, s obzirom na to da može izazvati društvenu osudu i dovesti do stigmatizacije odnosne osobe.

Usto, Sud smatra da, imajući u vidu osjetljivost tih podataka i ozbiljnost spomenutog zadiranja u dva navedena temeljna prava, ona imaju prednost i pred interesom javnosti za pristup službenim dokumentima, kao što je Nacionalni registar vozila i njihovih vozača, i pred pravom na slobodu informiranja.

Osim toga, zbog istih razloga Sud smatra da se OUZP-u protivi latvijski propis i u dijelu u kojem ovlašćuje CSDD da podatke o kaznenim bodovima izrečenima vozačima vozila za prometne prekršaje dostavi gospodarskim subjektima kako bi ih oni mogli ponovno upotrijebiti i priopćiti javnosti.

Naposljetku, Sud pojašnjava da se načelu nadređenosti prava Unije protivi to da sud koji je uputio zahtjev, postupajući po tužbi protiv latvijskog propisa za koji je Sud ocijenio da nije u skladu s pravom Unije, odluči da se pravni učinci tog propisa održavaju do dana donošenja njegove konačne presude.

III. Obrade osobnih podataka u smislu sektorskih propisa

1. Obrada osobnih podataka u sektoru elektroničkih komunikacija

Presuda od 2. listopada 2018. (veliko vijeće), Ministerio Fiscal (C-207/16, EU:C:2018:788)

U tom je predmetu španjolski istražni sud odbio zahtjev podnesen u okviru istrage o nasilnoj krađi novčanika i mobilnog telefona. Konkretnije, policija je od navedenog suda zatražila da joj odobri pristup identifikacijskim podacima korisnikâ telefonskih brojeva koji su aktivirani s ukradenog telefona u razdoblju od dvanaest dana počevši od dana krađe. Odbijanje se temeljilo na obrazloženju prema kojem činjenice koje su dovele do kaznene istrage nisu predstavljale „teško” kazneno djelo, odnosno, u skladu sa španjolskim pravom, kazneno djelo za koje je zaprijećena kazna zatvora u trajanju duljem od pet godina, s obzirom na to da je pristup identifikacijskim podacima moguć samo za tu vrstu kaznenog djela.

Nakon što je Sud podsjetio na to da je u okviru postupka kaznene istrage pristup javnih tijela osobnim podacima koje su zadržali pružatelji usluga elektroničkih komunikacija obuhvaćen područjem primjene Direktive 2002/58, on smatra da pristup podacima u svrhu identifikacije nositelja SIM kartica aktiviranih ukradenim mobilnim telefonom, poput njihovih imena, prezimena i, prema potrebi, adresa, predstavlja zadiranje u

temeljna prava na poštovanje privatnog života i zaštite podataka, sadržanih u Povelji, čak i ako ne postoje okolnosti na temelju kojih se takvo zadiranje može ocijeniti „ozbiljnim”, neovisno o tome jesu li podaci o privatnom životu osjetljivi odnosno jesu li zainteresirane osobe zbog tog zadiranja pretrpjele eventualne neugodnosti. Međutim, Sud naglašava da to zadiranje nije toliko ozbiljno da bi taj pristup u području sprečavanja, istrage, otkrivanja i progona kaznenih djela trebao biti ograničen na borbu protiv teških kaznenih djela. Naime, iako se u Direktivi 2002/58 taksativno navode ciljevi kojima se može opravdati nacionalni propis kojim se uređuje pristup državnih tijela dotičnim podacima i na taj način odstupa od načela povjerljivosti elektroničkih komunikacija, pri čemu taj pristup doista treba strogo odgovarati jednom od tih ciljeva, Sud napominje da, kad je riječ o cilju sprečavanja, istrage, otkrivanja i progona kaznenih djela, on tekstom Direktive 2002/58 nije ograničen na borbu protiv teških kaznenih djela, nego se spominju „kaznena djela” općenito.

U tom kontekstu Sud pojašnjava da, iako je u svojoj presudi Tele2 Sverige i Watson i dr.[45] smatrao da samo borba protiv teškog kriminaliteta može opravdati pristup državnih tijela osobnim podacima koje su zadržali pružatelji komunikacijskih usluga na temelju kojih je, ukupno gledajući, moguće izvući precizne zaključke o privatnom životu osoba o čijim je podacima riječ, takvo je tumačenje obrazloženo činjenicom da cilj propisa kojima se uređuje pitanje tog pristupa mora biti povezan s ozbiljnošću predmetnog zadiranja u temeljna prava koje takav pristup podrazumijeva. Stoga se, u skladu s načelom proporcionalnosti, ozbiljno zadiranje u tom području može opravdati samo ciljem borbe protiv kriminaliteta koji se također može okvalificirati „teškim”. Nasuprot tomu, kad zadiranje nije ozbiljno, taj se pristup može opravdati ciljem sprečavanja, istrage, otkrivanja i progona „kaznenih djela” općenito.

U ovom slučaju Sud smatra da se pristup samo podacima na koje se odnosi predmetni zahtjev ne može kvalificirati kao „ozbiljno” zadiranje u temeljna prava ispitanika jer ti podaci ne omogućuju donošenje preciznih zaključaka o njihovu privatnom životu. Sud je iz toga zaključio da zadiranje koje podrazumijeva pristup takvim podacima može biti opravdano ciljem sprečavanja, istrage, otkrivanja i progona „kaznenih djela” općenito, pri čemu nije potrebno da su ta kaznena djela okvalificirana kao „teška”.

Presude od 6. listopada 2020. (veliko vijeće), Privacy International (C-623/17, EU:C:2020:790) i La Quadrature du Net i dr. (C-511/18, C-512/18 i C-520/18, EU:C:2020:791)

Sudska praksa o zadržavanju osobnih podataka i pristupu tim podacima u području elektroničkih komunikacija, posebno presuda Tele2 Sverige i Watson i dr., u kojoj je Sud odlučio da države članice ne mogu pružateljima elektroničkih komunikacijskih usluga naložiti obvezu općeg i neselektivnog zadržavanja podataka o prometu i lokaciji, izazvala je određenu zabrinutost država članica, koje su se bojale da im je oduzet instrument koji smatraju nužnim za zaštitu nacionalne sigurnosti i borbu protiv kriminala.

[45] Presuda Suda od 21. prosinca 2016., Tele2 Sverige i Watson i dr. (C-203/15 i C-698/15, EU:C:2016:970)

S obzirom na tu pozadinu, pred Investigatory Powers Tribunalom (Sud za istražne ovlasti, Ujedinjena Kraljevina) (Privacy International, C-623/17), Conseilom d'État (Državno vijeće, Francuska) (La Quadrature du Net i dr., spojeni predmeti C-511/18 i C-512/18) kao i Courom constitutionnelle (Ustavni sud, Belgija) (Ordre des barreaux francophones et germanophone i dr., C-520/18) pokrenuti su postupci koji se tiču zakonitosti propisa određenih država članica u tim područjima koji predviđaju obvezu pružatelja elektroničkih komunikacijskih usluga prenošenja podataka tijelu javne vlasti ili obvezu općeg i neselektivnog zadržavanja podataka o prometu i lokaciji.

Dvjema presudama velikog vijeća objavljenima 6. listopada 2020. Sud presuđuje, prije svega, da su nacionalni propisi koji nalažu pružateljima elektroničkih komunikacijskih usluga da zadržavaju podatke o prometu i lokaciji ili pak da ih prenose sigurnosnim i obavještajnim nacionalnim tijelima obuhvaćeni područjem primjene Direktive 2002/58.

Nadalje, Sud podsjeća na to da Direktiva 2002/58[46] ne dopušta da odstupanje od načelne obveze jamčenja povjerljivosti elektroničkih komunikacija i podataka te zabrane pohrane tih podataka postane pravilo. Iz toga proizlazi da ta direktiva dopušta državama članicama da usvoje, između ostaloga, radi zaštite nacionalne sigurnosti, zakonske mjere usmjerene na ograničenje dosega prava i obveza predviđenih tom direktivom, posebno obveze jamčenja povjerljivosti komunikacija i podataka o prometu[47], jedino poštujući opća načela prava Unije, među kojima je načelo proporcionalnosti, kao i temeljna prava zajamčena Poveljom[48].

U tom kontekstu, Sud smatra, s jedne strane, u predmetu Privacy International, da se Direktivi 2002/58, tumačenoj u skladu s Poveljom, protivi nacionalni propis kojim se nalaže pružateljima elektroničkih komunikacijskih usluga, s ciljem zaštite nacionalne sigurnosti, opći i neselektivni prijenos podataka o prometu i lokaciji sigurnosnim i obavještajnim službama. S druge strane, u spojenim predmetima La Quadrature du Net i dr. kao i u predmetu Ordre des barreaux francophones et germanophone i dr. Sud procjenjuje da se toj istoj direktivi protive zakonodavne mjere koje nalažu pružateljima elektroničkih komunikacijskih usluga, u preventivne svrhe, opće i neselektivno zadržavanje podataka o prometu i lokaciji.

Naime, te obveze prijenosa te općeg i neselektivnog zadržavanja tih podataka predstavljaju osobito ozbiljno zadiranje u prava zajamčena Poveljom a da ponašanje osoba o čijim se podacima radi pritom nije povezano s ciljem koji se predmetnim propisom nastoji postići. Na sličan način, Sud tumači članak 23. stavak 1. OUZP-a, s obzirom na Povelju, na taj način da mu se protivi nacionalni propis kojim se nalaže pružateljima pristupa javnim internetskim komunikacijskim uslugama i pružateljima usluga smještaja sadržaja opće i neselektivno zadržavanje osobnih podataka koji se odnose na te usluge.

---

[46] Članak 15. stavci 1. i 3. Direktive 2002/58

[47] Članak 5. stavak 1. Direktive 2002/58

[48] Posebno članci 7., 8. i 11. kao i članak 52. stavak 1. Povelje

Nasuprot tomu, Sud smatra da se, u situacijama u kojima je dotična država članica suočena s ozbiljnom prijetnjom nacionalnoj sigurnosti koja se pokazala stvarnom i trenutačnom ili predvidljivom, Direktivi 2002/58, tumačenoj u skladu s Poveljom, ne protivi to da se pružateljima elektroničkih komunikacijskih usluga naloži opće i neselektivno zadržavanje podataka o prometu i lokaciji. U tom kontekstu, Sud pojašnjava da odluka kojom je predviđen takav nalog, izdan za razdoblje koje je vremenski ograničeno na ono što strogo nužno, mora biti predmet djelotvornog nadzora od strane suda ili neovisnog upravnog tijela čija odluka ima obvezujući učinak, a kojom se nastoji provjeriti postoji li jedna od tih situacija i poštuju li se uvjeti i jamstva koji se moraju predvidjeti. U tim istim okolnostima, navedenoj se direktivni ne protivi ni automatska analiza podataka, posebno onih o prometu i lokaciji, svih korisnika sredstava elektroničke komunikacije.

Sud dodaje da se Direktivi 2002/58, tumačenoj u skladu s Poveljom, ne protivi zakonska mjera koja omogućuje ciljano zadržavanje, za razdoblje koje je vremenski ograničeno na ono što je strogo nužno, podataka o prometu i lokaciji, koje je ograničeno na temelju objektivnih i nediskriminatornih kriterija, ovisno o kategorijama dotičnih osoba ili posredstvom zemljopisnog kriterija. Isto tako, ovoj direktivi se ne protive one mjere koje predviđaju opće i neselektivno zadržavanje IP adresa dodijeljenih izvoru veze, za razdoblje koje je vremenski ograničeno na ono što je strogo nužno, niti one koje predviđaju takvo zadržavanje podataka o građanskom identitetu korisnika elektroničkih komunikacijskih sredstava, u kojem slučaju države članice nisu obvezne vremenski ograničiti zadržavanje. Štoviše, navedenoj se direktivi ne protivi zakonska mjera koja omogućuje žurno zadržavanje podataka kojima raspolažu pružatelji usluga u situacijama iz kojih proizlazi nužda njihova zadržavanja preko zakonskih rokova zadržavanja, za potrebe rasvjetljavanja teških kaznenih djela ili ugroza nacionalne sigurnosti, i to kako u situaciji u kojoj su ta kaznena djela ili te ugroze već mogli biti utvrđeni tako i u situaciji u kojoj se može osnovano sumnjati u njihovo postojanje.

Nadalje, Sud navodi da se Direktivi 2002/58, tumačenoj u skladu s Poveljom, ne protivi nacionalni propis koji nalaže pružateljima elektroničkih komunikacijskih usluga prikupljanje u stvarnom vremenu podataka o prometu i lokaciji, ako je to prikupljanje ograničeno na osobe za koje postoji valjan razlog za sumnju da su na bilo koji način uključene u terorističke aktivnosti i ako je podvrgnuto prethodnom nadzoru suda ili neovisnog upravnog tijela čija odluka ima obvezujući učinak, pri čemu se taj sud ili tijelo moraju uvjeriti da je takvo prikupljanje u stvarnom vremenu odobreno samo u granicama onog što je strogo nužno. U slučaju hitnosti, nadzor mora uslijediti u kratkim rokovima.

Naposljetku, Sud razmatra pitanje održavanja na snazi učinaka nacionalnog zakonodavstva za koje je presuđeno da je suprotno pravu Unije. U tom pogledu, Sud smatra da nacionalni sud ne može primijeniti odredbu svojeg nacionalnog prava koja ga ovlašćuje da vremenski ograniči učinke utvrđenja nezakonitosti koje mora iznijeti na temelju tog prava u pogledu nacionalnog propisa kojim se pružateljima elektroničkih komunikacijskih usluga nalaže općenito i neselektivno zadržavanje podataka o prometu i

lokaciji, za koje je presuđeno da nije u skladu s Direktivom 2002/58, tumačenom u skladu s Poveljom.

S obzirom na navedeno i radi davanja korisnog odgovora nacionalnom sudu, Sud podsjeća na to da je u trenutačnom stanju prava Unije u načelu samo na nacionalnom pravu da odredi pravila o dopuštenosti i ocjeni, u okviru kaznenog postupka pokrenutog protiv osoba osumnjičenih za teška kaznena djela, onih informacija i dokaza koji su pribavljeni takvim zadržavanjem podataka suprotnim pravu Unije. Međutim, Sud pojašnjava da Direktiva 2002/58, tumačena u skladu s načelom djelotvornosti, nalaže nacionalnom kaznenom sudu da, u okviru takvog kaznenog postupka, izdvoji dokaze koji su pribavljeni općim i neselektivnim zadržavanjem podataka o prometu i lokaciji nespojivim s pravom Unije, ako osobe osumnjičene za kaznena djela nisu u mogućnosti učinkovito se izjasniti o tim dokazima.

Presuda od 2. ožujka 2021. (veliko vijeće), Prokuratuur (Uvjeti pristupa podacima o elektroničkim komunikacijama) (C-746/18, EU:C:2021:152)

Protiv osobe H. K. u Estoniji je pokrenut kazneni postupak zbog krađe, korištenja bankovnom karticom treće osobe i nasilja prema osobama koje sudjeluju u sudskom postupku. Osobu H. K. je prvostupanjski sud zbog tih kaznenih djela osudio na kaznu zatvora od dvije godine. Ta je odluka zatim potvrđena u žalbenom postupku. Zapisnici na kojima se temelji utvrđenje počinjenja tih kaznenih djela sastavljeni su, među ostalim, na temelju osobnih podataka dobivenih u okviru pružanja elektroničkih komunikacijskih usluga. Riigikohus (Vrhovni sud, Estonija), kojem je osoba H. K. podnijela žalbu u kasacijskom postupku, iznio je sumnje u pogledu usklađenosti s pravom Unije[49] uvjeta u kojima su istražne službe imale pristup tim podacima.

Te su se sumnje, kao prvo, odnosile na pitanje je li trajanje razdoblja za koje su istražne službe imale pristup podacima kriterij na temelju kojeg se može ocijeniti ozbiljnost zadiranja u temeljna prava dotičnih osoba koje čini taj pristup. Tako se, kada je to razdoblje vrlo kratko ili je količina prikupljenih podataka vrlo ograničena, sud koji je uputio zahtjev pita može li cilj borbe protiv kriminaliteta općenito, a ne samo protiv teških kaznenih djela opravdati takvo zadiranje. Kao drugo, sud koji je uputio zahtjev ima sumnje u vezi s mogućnosti da se estonsko državno odvjetništvo, imajući u vidu različite zadaće koje su mu dodijeljene nacionalnim pravom, smatra „neovisnim" upravnim tijelom u smislu presude Tele2 Sverige i Watson i dr.[50], koje tijelu nadležnom za provedbu istrage može odobriti pristup dotičnim podacima.

Svojom presudom, donesenom u velikom vijeću, Sud presuđuje da se Direktivi 2002/58, u vezi s Poveljom, protivi nacionalni propis koji omogućuje pristup državnih tijela podacima o prometu ili podacima o lokaciji, koji mogu pružiti informacije o komunikacijama koje izvršava korisnik sredstva elektroničke komunikacije ili o lokaciji

[49] Preciznije, s člankom 15. stavkom 1. Direktive 2002/58, u vezi s člancima 7., 8. i 11. kao i člankom 52. stavkom 1. Povelje

[50] Presuda od 21. prosinca 2016., Tele2 Sverige i Watson i dr. (C-203/15 i C-698/15, EU:C:2016:970, t. 120.)

terminalne opreme kojom se koristi i omogućiti izvođenje preciznih zaključaka o njegovu privatnom životu, u svrhu sprečavanja, istrage, otkrivanja ili progona kaznenih djela, a da taj pristup nije ograničen na postupke kojima je cilj borba protiv teških kaznenih djela ili sprečavanje ozbiljnih prijetnji javnoj sigurnosti. Prema mišljenju Suda, trajanje razdoblja za koje se traži pristup tim podacima i količina ili priroda podataka dostupnih u odnosu na takvo razdoblje nema utjecaja u tom pogledu. Usto, Sud smatra da se toj istoj direktivi, u vezi s Poveljom, protivi nacionalni propis kojim se državnom odvjetništvu dodjeljuje nadležnost za odobravanje pristupa državnog tijela podacima o prometu i podacima o lokaciji radi vođenja kaznene istrage.

Što se tiče cilja sprečavanja, istrage, otkrivanja ili progona kaznenih djela, koji slijedi propis o kojem je riječ u glavnom postupku, Sud smatra da u skladu s načelom proporcionalnosti samo ciljevi borbe protiv teških kaznenih djela ili sprečavanje ozbiljnih prijetnji javnoj sigurnosti mogu opravdati pristup državnih tijela skupu podataka o prometu ili podataka o lokaciji, koji mogu omogućiti izvođenje preciznih zaključaka o privatnom životu dotičnih osoba, a drugi čimbenici, koji se odnose na proporcionalnost zahtjeva za pristup, poput trajanja razdoblja za koje se pristup takvim podacima traži, ne mogu imati za posljedicu to da cilj sprečavanja, istrage, otkrivanja i progona kaznenih djela općenito može opravdati takav pristup.

Kad je riječ o nadležnosti dodijeljenoj državnom odvjetništvu za odobravanje pristupa državnog tijela podacima o prometu i podacima o lokaciji radi vođenja kaznene istrage, Sud podsjeća na to da je na nacionalnom pravu utvrđivanje uvjeta u kojima pružatelji elektroničkih komunikacijskih usluga moraju odobriti nadležnim nacionalnim tijelima pristup podacima kojima raspolažu. Međutim, da bi ispunio zahtjev proporcionalnosti, takav propis mora sadržavati jasna i precizna pravila o dosegu i primjeni dotične mjere te propisivati minimalne uvjete, na način da osobe o čijim je osobnim podacima riječ raspolažu dostatnim jamstvima koja omogućuju učinkovitu zaštitu tih podataka od rizika zlouporabe. Taj propis mora biti zakonski obvezujući u unutarnjem pravu i navoditi u kojim se okolnostima i pod kojim uvjetima mjera kojom se predviđa obrada takvih podataka može donijeti, jamčeći time da će zadiranje biti ograničeno na ono što je strogo nužno.

Sud smatra da je u svrhu osiguranja punog poštovanja tih uvjeta u praksi bitno da se prije pristupa nadležnih nacionalnih tijela zadržanim podacima provede nadzor suda ili neovisnog upravnog tijela i da odluka tog suda ili tijela bude donesena nakon obrazloženog zahtjeva tih tijela podnesenog osobito u okviru postupaka sprečavanja, otkrivanja ili progona kaznenih djela. U slučaju opravdane hitnosti nadzor mora uslijediti u kratkim rokovima.

U tom pogledu Sud pojašnjava da taj prethodni nadzor među ostalim zahtijeva da sud ili tijelo zaduženo za izvršavanje tog nadzora raspolaže svim ovlastima i pruža sva potrebna jamstva za usklađivanje različitih interesa i prava o kojima je riječ. Konkretnije, kad je riječ o kaznenoj istrazi, takav nadzor zahtijeva da taj sud ili to tijelo može osigurati pravednu ravnotežu između, s jedne strane, interesa povezanih s potrebama istrage u okviru borbe protiv kriminaliteta i, s druge strane, temeljnih prava na poštovanje privatnog života i zaštite osobnih podataka osoba čiji su podaci obuhvaćeni pristupom.

Kada taj nadzor ne izvršava sud nego neovisno upravno tijelo, ono mora uživati položaj koji mu omogućava da prilikom obavljanja svojih zadaća postupa objektivno i nepristrano i u tu svrhu mora biti zaštićeno od svakog vanjskog utjecaja.

Sud smatra da iz toga proizlazi da zahtjev neovisnosti koji mora ispuniti tijelo zaduženo za obavljanje prethodnog nadzora nalaže da to tijelo ima svojstvo treće strane u odnosu na ono koje zahtijeva pristup podacima, tako da prvonavedeno tijelo može izvršavati taj nadzor objektivno i nepristrano i zaštićeno od svakog vanjskog utjecaja. Konkretno, zahtjev neovisnosti u kaznenom postupku podrazumijeva da tijelo zaduženo za taj prethodni nadzor, s jedne strane, nije uključeno u provođenje predmetne kaznene istrage i, s druge strane, da ima neutralan položaj u odnosu na stranke kaznenog postupka. Međutim, to nije tako u slučaju državnog odvjetništva koje, poput estonskog državnog odvjetništva, vodi istragu i, ovisno o slučaju, zastupa optužbu. Iz toga proizlazi da državno odvjetništvo nije u položaju izvršavati navedeni prethodni nadzor.

Presuda od 5. travnja 2022. (veliko vijeće), Commissioner of An Garda Síochána i dr. (C-140/20, EU:C:2022:258)

U tom predmetu zahtjev za prethodnu odluku podnio je Supreme Court (Vrhovni sud, Irska) u okviru građanskog postupka koji je pokrenula osoba osuđena na doživotni zatvor za ubojstvo počinjeno u Irskoj. Ta je osoba osporavala usklađenost s pravom Unije određenih odredbi nacionalnog zakona o zadržavanju podataka dobivenih u vezi s elektroničkim komunikacijama. Na temelju tog zakona pružatelji elektroničkih komunikacijskih usluga zadržali su i učinili dostupnim policijskim tijelima podatke o prometu i lokaciji u vezi s telefonskim podacima okrivljenika. Dvojbe suda koji je uputio zahtjev odnosile su se, među ostalim, na usklađenost sustava općeg i neselektivnog zadržavanja tih podataka u vezi s borbom protiv teških kaznenih djela s Direktivom 2002/58, u vezi s Poveljom.

Svojom presudom, donesenom u velikom vijeću, Sud potvrđuje, pojašnjavajući njezin doseg, sudsku praksu proizišlu iz presude La Quadrature du Net i dr.[51], podsjećajući na to da opće i neselektivno zadržavanje podataka o prometu i lokaciji nije dopušteno u svrhe borbe protiv teških kaznenih djela i sprečavanja ozbiljnih prijetnji javnoj sigurnosti. Također potvrđuje sudsku praksu proizišlu iz presude Prokuratuur (Uvjeti pristupa podacima o elektroničkim komunikacijama)[52], osobito u pogledu obveze uvjetovanja pristupa nadležnih nacionalnih tijela navedenim zadržanim podacima prethodnim nadzorom u pogledu policijskog službenika koji izvršava sud ili neovisno upravno tijelo.

Sud kao prvo presuđuje da se Direktivi 2002/58, u vezi s Poveljom, protive zakonske mjere kojima se, u svrhe borbe protiv teških kaznenih djela i sprečavanja ozbiljnih prijetnji javnoj sigurnosti, predviđa opće i neselektivno zadržavanje podataka o prometu i lokaciji. Naime, vodeći računa, s jedne strane, o odvraćajućim učincima na korištenje

[51] Presuda od 6. listopada 2020., La Quadrature du Net i dr. (C-511/18, C-512/18 i C-520/18, EU:C:2020:791)

[52] Presuda od 2. ožujka 2021., Prokuratuur (Uvjeti pristupa podacima o elektroničkim komunikacijama) (C-746/18, EU:C:2021:152)

temeljnim pravima[53] do kojih može dovesti to zadržavanje i, s druge strane, o ozbiljnosti zadiranja koje ono podrazumijeva, takvo zadržavanje mora biti iznimka, a ne pravilo u sustavu uspostavljenom Direktivom 2002/58 i ti podaci ne mogu biti predmet sustavnog i kontinuiranog zadržavanja. Kaznena djela, čak ni osobito teška, ne mogu se izjednačiti s prijetnjom nacionalnoj sigurnosti jer bi se takvim izjednačavanjem mogla unijeti u kategoriju koja se nalazi između nacionalne i javne sigurnosti, kako bi se na drugu kategoriju mogli primijeniti zahtjevi koji su svojstveni prvoj.

Nasuprot tomu, Direktivi 2002/58, u vezi s Poveljom, ne protivi se, u svrhe borbe protiv teških kaznenih djela i sprečavanja ozbiljnih prijetnji javnoj sigurnosti, ciljano zadržavanje podataka o prometu i lokaciji koje je ograničeno na temelju objektivnih i nediskriminatornih kriterija, ovisno o kategorijama dotičnih osoba ili posredstvom zemljopisnog kriterija, za razdoblje koje je vremenski ograničeno na ono što je strogo nužno, ali se može produljiti. Dodaje da takva mjera zadržavanja koja obuhvaća mjesta ili infrastrukturu u koje često zalazi povećan broj osoba ili strateška mjesta poput zračnih luka, kolodvora, morskih luka ili naplatnih postaja, omogućava nadležnim tijelima da prikupe podatke o prisutnosti, u tim mjestima ili zemljopisnim područjima, osoba koje u njima koriste sredstvo elektroničke komunikacije i iz tih podataka donesu zaključke o njihovoj prisutnosti i njihovoj aktivnosti u navedenim mjestima ili u zemljopisnim područjima u svrhe borbe protiv teških kaznenih djela. U svakom slučaju, moguće postojanje poteškoća za precizno definiranje slučajeva i uvjeta u kojima ciljano zadržavanje može biti izvršeno ne može opravdati to da države članice, time što iznimku učine pravilom, predvide općenito i neselektivno zadržavanje podataka o prometu i podataka o lokaciji.

Toj direktivi, u vezi s Poveljom, ne protive se ni zakonske mjere kojima se u iste svrhe predviđa opće i neselektivno zadržavanje IP adresa dodijeljenih izvoru veze, za razdoblje koje je vremenski ograničeno na ono što je strogo nužno te podataka o građanskom identitetu korisnika elektroničkih komunikacija. Što se tiče potonjeg aspekta, Sud konkretnije pojašnjava da se ni Direktivi 2002/58 ni bilo kojem drugom aktu prava Unije ne protivi nacionalno zakonodavstvo koje za cilj ima borbu protiv teških kaznenih djela, na temelju kojeg je kupnja sredstva elektroničke komunikacije poput *prepaid* SIM kartice uvjetovana provjerom službenih dokumenata kojima se utvrđuje građanski identitet kupca te registracijom, od strane prodavatelja, informacija koje iz toga proizlaze, a prodavatelj je po potrebi dužan dati pristup tim informacijama nadležnim nacionalnim tijelima.

Ništa drukčije nije u pogledu zakonskih mjera kojima se u svrhe borbe protiv teških kaznenih djela i sprečavanja ozbiljnih prijetnji nacionalnoj sigurnost predviđa korištenje naloga pružateljima elektroničkih komunikacijskih usluga na temelju odluke nadležnog tijela, podložne djelotvornom sudskom nadzoru, da u određenom trajanju hitno zadrže (*quick freeze*) podatke o prometu i lokaciji kojima ti pružatelji usluga raspolažu. Naime,

[53] Utvrđeni u člancima 7. do 11. Povelje

samo borba protiv teških kaznenih djela i, *a fortiori*, zaštita nacionalne sigurnosti mogu opravdati takvo zadržavanje, pod uvjetom da ta mjera i pristup zadržanim podacima poštuju granice strogo nužnog. Sud podsjeća na to da se takva mjera hitnog zadržavanja može proširiti na podatke o prometu i lokaciji u vezi s osobama različitima od onih koje su osumnjičene da su planirale ili počinile teško kazneno djelo ili da su ugrozile nacionalnu sigurnost, pod uvjetom da ti podaci mogu, na temelju objektivnih i nediskriminatornih kriterija, doprinijeti rasvjetljavanju takvog djela ili takve ugroze nacionalne sigurnosti, poput podataka o njezinoj žrtvi, društvenom i poslovnom okružju.

Međutim, sud potom navodi da sve navedene zakonske mjere moraju osigurati jasnim i preciznim pravilima da predmetno zadržavanje podataka podliježe poštovanju s time povezanih materijalnih i postupovnih uvjeta te da dotične osobe imaju djelotvorna jamstva protiv rizika od zlouporabe. Različite mjere zadržavanja podataka o prometu i podataka o lokaciji mogu se, ovisno o izboru nacionalnog zakonodavca i poštujući granice strogo nužnog, primijeniti zajedno.

Usto Sud pojašnjava da bi dopustiti, u svrhe borbe protiv teških kaznenih djela, pristup takvim zadržanim podacima općenito i neselektivno, kako bi se suočilo s ozbiljnom prijetnjom za nacionalnu sigurnost, bilo protivno hijerarhiji ciljeva od općeg interesa koji mogu opravdati mjeru poduzetu na temelju Direktive 2002/58. Naime, time bi se dopustilo da se pristup može opravdati ciljem koji je manje važan od onog kojim se opravdava zadržavanje, odnosno zaštitom nacionalne sigurnosti, čime bi se moglo oduzeti svaki koristan učinak zabrani općeg i neselektivnog zadržavanja u svrhe borbe protiv teških kaznenih djela.

Kao drugo, Sud odlučuje da se Direktivi 2002/58, u vezi s Poveljom, protivi nacionalni propis na temelju kojeg je odgovornost za centraliziranu obradu zahtjeva za pristup podacima koje su zadržali pružatelji elektroničkih komunikacijskih usluga, koje podnosi policija u okviru istraživanja i progona teških kaznenih djela, na policijskom službeniku, kojem pomaže jedinica uspostavljena unutar policije koja uživa određeni stupanj autonomije prilikom obavljanja svoje zadaće i čije odluke kasnije mogu biti predmet sudskog nadzora. Naime, s jedne strane, takav službenik ne ispunjava zahtjeve neovisnosti i nepristranosti koji su nužni za upravno tijelo koje izvršava prethodni nadzor zahtjeva za pristup podacima koje su podnijela nadležna nacionalna tijela jer nema svojstvo treće strane u odnosu na ta tijela. S druge strane, iako odluka takvog službenika može biti predmet naknadnog sudskog nadzora, taj nadzor ne može zamijeniti neovisan i, osim u slučaju valjano opravdane hitnosti, prethodni nadzor.

Naposljetku, kao treće, Sud potvrđuje svoju sudsku praksu prema kojoj se pravu Unije protivi to da nacionalni sud vremenski ograniči učinke utvrđenja nevaljanosti, koje je na njemu na temelju nacionalnog prava, u pogledu nacionalnog zakonodavstva kojim se pružateljima elektroničkih komunikacijskih usluga nalaže opće i neselektivno zadržavanje podataka o prometu i podataka o lokaciji, zbog neusklađenosti tog zakonodavstva s Direktivom 2002/58. Stoga Sud podsjeća na to da dopuštenost dokaza dobivenih takvim zadržavanjem, u skladu s načelom postupovne autonomije država

članica, proizlazi iz nacionalnog prava, pod uvjetom poštovanja osobito načela ekvivalentnosti i djelotvornosti.

Presuda od 20. rujna 2022. (veliko vijeće), VD i SR (C-339/20 i C-397/20, EU:C:2022:703)

Nakon istrage Autoritéa des marchés financiers (Tijelo za financijska tržišta, AMF, Francuska) pokrenuti su kazneni postupci protiv VD i SR, dviju fizičkih osoba optuženih za kaznena djela trgovanja na temelju povlaštenih informacija, prikrivanja tog trgovanja, sudioništva, korupcije i pranja novca. U okviru te istrage AMF je upotrijebio osobne podatke iz telefonskih poziva osoba VD i SR nastale na temelju francuskog code des postes et des communications électroniques (Zakonik o poštanskim uslugama i elektroničkim komunikacijama) u okviru pružanja elektroničkih komunikacijskih usluga.

Budući da se provođenje istrage protiv njih temeljilo na podacima o prometu koje je pružio AMF, osobe VD i SR podnijele su tužbu Couru d'appel de Paris (Žalbeni sud u Parizu, Francuska), pozivajući se, među ostalim, na tužbeni razlog koji se temeljio na povredi članka 15. stavka 1. Direktive 2002/58 u vezi s člancima 7., 8. i 11. te člankom 52. stavkom 1. Povelje. Konkretnije, pozivajući se na sudsku praksu proizišlu iz presude Tele2 Sverige i Watson i dr.[54] osobe VD i SR osporavale su činjenicu da je AMF prikupio navedene podatke na temelju dotičnih nacionalnih odredbi, iako te odredbe, s jedne strane, nisu bile u skladu s pravom Unije jer su predviđale opće i neselektivno zadržavanje podataka o vezi i, s druge strane, nisu određivale nikakve granice ovlasti AMF-ovih istražitelja da ishode dostavu zadržanih podataka.

Dvjema presudama, od 20. prosinca 2018. i od 7. ožujka 2019., Cour d'appel de Paris (Žalbeni sud u Parizu) odbio je tužbe osoba VD i SR. Kako bi odbili gore navedeni tužbeni razlog, suci koji odlučuju o meritumu donijeli su zaključak na temelju, među ostalim, činjenice da Uredba o zlouporabi tržišta[55] dopušta nadležnim tijelima da, u mjeri u kojoj je to dopušteno prema nacionalnom pravu, zahtijevaju postojeće zapise o podatkovnom prometu koje posjeduju telekomunikacijski operateri, kada postoji sumnja u povredu zabrane trgovanja na temelju povlaštenih informacija i kada takvi zapisi mogu biti relevantni za istragu o toj povredi.

Osobe VD i SR potom su podnijele žalbu Couru de cassation (Kasacijski sud, Francuska), sudu koji je uputio zahtjev u ovim predmetima.

U tom kontekstu taj se sud pita o usklađenosti članka 15. stavka 1. Direktive 2002/58, u vezi s Poveljom, sa zahtjevima koji proizlaze iz članka 12. stavka 2. točaka (a) i (d) Direktive o zlouporabi tržišta[56] i članka 23. stavka 2. točaka (g) i (h) Uredbe o zlouporabi

---

54 Presuda od 21. prosinca 2016., Tele2 Sverige i Watson i dr. (C-203/15 i C-698/15, EU:C:2016:970)

55 Uredba (EU) br. 596/2014 Europskog parlamenta i Vijeća od 16. travnja 2014. o zlouporabi tržišta (Uredba o zlouporabi tržišta) te stavljanju izvan snage Direktive 2003/6 i direktiva Komisije 2003/124/EZ, 2003/125/EZ i 2004/72/EZ (SL 2014., L 173, str. 1. i ispravak SL 2016., L 287, str. 320.)

56 Direktiva 2003/6/EZ Europskog parlamenta i Vijeća od 28. siječnja 2003. o trgovanju na temelju povlaštenih informacija i manipuliranju tržištem (zlouporabi tržišta) (SL 2003., L 96, str. 16.) (SL, posebno izdanje na hrvatskom jeziku, poglavlje 6., svezak 3., str. 74.)

tržišta. To pitanje proizlazi iz zakonodavnih mjera o kojima je riječ u glavnom postupku, kojima se za operatore elektroničkih komunikacijskih usluga u svrhu borbe protiv kaznenih djela zlouporaba tržišta, među kojima je trgovanje na temelju povlaštenih informacija, preventivno predviđa opće i neselektivno zadržavanje podataka o prometu tijekom jedne godine od dana zapisa. Ako bi Sud smatrao da zakonodavstvo o zadržavanju podataka o vezi o kojem je riječ u glavnim postupcima nije u skladu s pravom Unije, postavlja se pitanje privremenog zadržavanja učinaka tog zakonodavstva kako bi se izbjegla pravna nesigurnost i omogućilo da se prethodno prikupljeni i zadržani podaci upotrijebe u svrhu otkrivanja i progona trgovanja na temelju povlaštenih informacija.

U svojoj presudi Sud, zasjedajući u velikom vijeću, presuđuje da nije dopušteno preventivno opće i neselektivno zadržavanje podataka o prometu koje provode operatori elektroničkih komunikacijskih usluga tijekom jedne godine od dana zapisa u svrhu borbe protiv kaznenih djela zlouporaba tržišta. Osim toga, on potvrđuje svoju sudsku praksu prema kojoj se pravu Unije protivi to da nacionalni sud vremenski ograniči učinke proglašenja nevaljanosti koju je on dužan utvrditi u pogledu nacionalnih zakonodavnih odredbi nespojivih s pravom Unije.

Sud najprije podsjeća na to da prilikom tumačenja odredbe prava Unije valja uzeti u obzir ne samo njezin tekst nego i kontekst u kojemu se nalazi te ciljeve propisa kojeg je dio.

Što se tiče teksta odredbi navedenih u prethodnim pitanjima, Sud utvrđuje da, dok se članak 12. stavak 2. točka (d) Direktive o zlouporabi tržišta odnosi na AMF-ovu ovlast u pogledu „traženja postojećih zapisa telefonskih razgovora i postojećih zapisa o prijenosu podataka”, članak 23. stavak 2. točke (g) i (h) Uredbe o zlouporabi tržišta upućuje na ovlast tog tijela da zahtijeva, s jedne strane, „zapise […] o podatkovnom prometu koje posjeduju investicijska društva, kreditne institucije ili financijske institucije” i, s druge strane, „u mjeri u kojoj je to dopušteno prema nacionalnom pravu, […] postojeće zapise o podatkovnom prometu koje posjeduje telekomunikacijski operater”. Prema mišljenju Suda, iz teksta tih odredbi nedvojbeno proizlazi da se njima AMF-ova ovlast ograničava samo na to da on „traži” ili „zahtijeva” podatke koje posjeduju ti operatori, što odgovara pristupu tim podacima. Osim toga, upućivanje na „postojeće” zapise, koje „posjeduju” navedeni operatori, upućuje na to da zakonodavac Unije nije namjeravao urediti mogućnost da nacionalni zakonodavac uspostavi obvezu zadržavanja takvih zapisa. Prema mišljenju Suda, to tumačenje, osim toga, potvrđuju kontekst u kojem se nalaze navedene odredbe kao i zadani ciljevi propisa kojeg su te iste odredbe dio.

Što se tiče konteksta u kojem se nalaze odredbe na koje se odnose prethodna pitanja, Sud primjećuje da, iako je, u skladu s relevantnim odredbama Direktive o zlouporabi tržišta i Uredbe o zlouporabi tržišta[57] zakonodavac Unije namjeravao državama

[57] Članak 12. stavak 1. Direktive o zlouporabi tržišta odnosno članak 23. stavak 3. Uredbe o zlouporabi tržišta, u vezi s njezinom uvodnom izjavom 62.

članicama nametnuti obvezu da poduzmu potrebne mjere kako bi nadležna tijela u području financija raspolagala nizom prikladnih alata, nadležnosti i resursa kao i ovlastima nadzora i istrage koje su potrebne za osiguranje učinkovitosti njihovih zadaća, te se odredbe ne izjašnjavaju ni o eventualnoj mogućnosti država članica da u tu svrhu uspostave, na teret operatora elektroničkih komunikacijskih usluga, obvezu općeg i neselektivnog zadržavanja podataka o prometu ni o uvjetima pod kojima te podatke mogu zadržavati ti operatori u svrhu njihove predaje, prema potrebi, nadležnim tijelima.

Kad je riječ o ciljevima koji se žele postići predmetnim propisima, Sud navodi da i iz Direktive o zlouporabi tržišta i iz Uredbe o zlouporabi tržišta[58] proizlazi da je cilj tih instrumenata osigurati integritet financijskih tržišta Unije i povećati povjerenje ulagateljâ u ta tržišta, pri čemu to povjerenje počiva, među ostalim, na činjenici da će biti u ravnopravnom položaju zaštićenom od nezakonite upotrebe povlaštenih informacija. Svrha zabrane trgovanja na temelju povlaštenih informacija propisane tim instrumentima[59] jest osigurati jednakost između suugovaratelja u burzovnoj transakciji i pritom izbjeći da se jedan od njih, koji posjeduje povlaštenu informaciju i zbog toga je u povlaštenom položaju u odnosu na druge ulagatelje, njome okoristi na štetu onih koji je nemaju. Iako su u skladu s Uredbom o zlouporabi tržišta[60], zapisi podataka o vezi ključan, a ponekad i jedini dokaz kojim se može otkriti i dokazati postojanje trgovanja na temelju povlaštenih informacija i manipuliranja tržištem, ta se uredba ipak odnosi samo na zapise koje „posjeduju” operatori elektroničkih komunikacijskih usluga kao i na ovlast nadležnog tijela u području financija da od tih operatora „zahtijevaju” dostavu „postojećih” podataka. Stoga iz tog teksta ni na koji način ne proizlazi da je zakonodavac Unije tom uredbom namjeravao državama članicama priznati ovlast da operatorima elektroničkih komunikacijskih usluga nametnu opću obvezu zadržavanja podataka. Iz toga slijedi da ni Direktiva o zlouporabi tržišta ni Uredba o zlouporabi tržišta ne mogu činiti pravnu osnovu opće obveze zadržavanja zapisa podataka o prometu koje posjeduju operatori elektroničkih komunikacijskih usluga u svrhu izvršavanja ovlasti dodijeljenih nadležnom tijelu u području financija na temelju tih akata.

Nadalje, Sud podsjeća na to da je Direktiva 2002/58 referentni akt u području zadržavanja i, općenitije, obrade osobnih podataka u sektoru elektroničkih komunikacija, tako da tumačenje s obzirom na tu direktivu uređuje i zapise podataka o prometu koje posjeduju operatori elektroničkih komunikacijskih usluga, a koje nadležna tijela u području financija u smislu Direktive o zlouporabi tržišta i Uredbe o zlouporabi tržišta[61] mogu od njih zahtijevati. Ocjenu zakonitosti obrade zapisa koje posjeduju operatori elektroničkih komunikacijskih usluga[62] treba provesti s obzirom na uvjete predviđene Direktivom 2002/58 kao i na tumačenje te direktive u sudskoj praksi Suda.

---

58 Uvodne izjave 2. i 12. Direktive o zlouporabi tržišta odnosno članak 1. Uredbe o zlouporabi tržišta, u vezi s njezinim uvodnim izjavama 2. i 24.

59 Članak 2. stavak 1. Direktive o zlouporabi tržišta i članak 8. stavak 1. Uredbe o zlouporabi tržišta

60 Uvodna izjava 62. Uredbe o zlouporabi tržišta

61 Članak 11. Direktive o zlouporabi tržišta odnosno članak 22. Uredbe o zlouporabi tržišta

62 U smislu članka 12. stavka 2. točke (d) Direktive o zlouporabi tržišta i članka 23. stavka 2. točaka (g) i (h) Uredbe o zlouporabi tržišta

Stoga Sud presuđuje da se Direktivi 2002/58 i Uredbi o zlouporabi tržišta, u vezi s Direktivom o privatnosti i elektroničkim komunikacijama i Poveljom, protive zakonodavne mjere kojima se u svrhu borbe protiv kaznenih djela zlouporaba tržišta, među kojima je trgovanje na temelju povlaštenih informacija, preventivno predviđa privremeno opće i neselektivno zadržavanje podataka o prometu tijekom jedne godine od dana zapisa koje provode operatori elektroničkih komunikacijskih usluga.

Naposljetku, Sud potvrđuje svoju sudsku praksu prema kojoj se pravu Unije protivi to da nacionalni sud vremenski ograniči učinke proglašenja nevaljanosti koju je on dužan utvrditi, na temelju nacionalnog prava, u pogledu nacionalnih odredbi koje, s jedne strane, operatorima elektroničkih komunikacijskih usluga nalažu opće i neselektivno zadržavanje podataka o prometu i, s druge strane, dopuštaju dostavu takvih podataka nadležnom tijelu u području financija bez prethodnog odobrenja suda ili neovisnog upravnog tijela, zbog neusklađenosti tih odredbi s Direktivom 2002/58, u vezi s Poveljom. Stoga Sud podsjeća na to da dopuštenost dokaza dobivenih takvim zadržavanjem, u skladu s načelom postupovne autonomije država članica, proizlazi iz nacionalnog prava, pod uvjetom poštovanja osobito načela ekvivalentnosti i djelotvornosti. To načelo zahtijeva od nacionalnog kaznenog suda da izuzme informacije i dokaze koji su prikupljeni putem općeg i neselektivnog zadržavanja koje nije u skladu s pravom Unije ako dotične osobe ne mogu učinkovito komentirati te informacije i dokaze koji potječu iz područja koje je izvan poznavanja sudaca i koji mogu imati odlučujući utjecaj na ocjenu činjenica.

Presuda od 30. travnja 2024. (puni sastav), La Quadrature du Net i dr. (Osobni podaci i borba protiv povreda) (C-470/21, EU:C:2024:370)

Odlučujući o zahtjevu za prethodnu odluku koji je uputio Conseil d'État (Državno vijeće, Francuska), puni sastav Suda razvija svoju sudsku praksu u vezi s Direktivom 2002/58 pojašnjavajući, s jedne strane, uvjete pod kojima se može smatrati da opće zadržavanje IP adresa koje provode pružatelji elektroničkih komunikacijskih usluga nije ozbiljno zadiranje u prava na poštovanje privatnosti, zaštitu osobnih podataka i slobodu izražavanja koja su zajamčena Poveljom[63], kao i, s druge strane, mogućnost da javno tijelo pristupi određenim osobnim podacima koji su zadržani uz poštovanje tih uvjeta u okviru borbe protiv povreda prava intelektualnog vlasništva na internetu.

U predmetnom slučaju četiri su udruge Premier ministreu (predsjednik Vlade, Francuska) podnijele zahtjev za stavljanje izvan snage uredbe o automatskoj obradi

[63] Članci 7., 8. i 11. Povelje

osobnih podataka[64]. Budući da o tom zahtjevu nije donesena odluka, te su udruge Državnom vijeću podnijele tužbu za poništenje te implicitne odluke o odbijanju. Prema njihovu mišljenju, ta uredba i odredbe koje čine njezinu pravnu osnovu [65] povređuju pravo Unije.

Na temelju francuskog zakonodavstva Haute Autorité pour la diffusion des œuvres et la protection des droits sur internet (Visoko tijelo za emitiranje djelâ i zaštitu prava na internetu, Francuska, u daljnjem tekstu: Hadopi), kako bi moglo identificirati osobe odgovorne za povrede autorskih ili srodnih prava koje su počinjene na internetu, ovlašten je pristupiti određenim podacima koje su pružatelji elektroničkih komunikacijskih usluga dužni zadržati. Ti se podaci odnose na građanski identitet određene osobe koji odgovaraju njezinoj IP adresi koju su prethodno prikupile organizacije nositeljâ prava. Kada je identificiran nositelj IP adrese upotrijebljene za aktivnosti kojima se počinila takva povreda, Hadopi slijedi postupak „postupnog odgovora". Konkretnije, on je ovlašten toj osobi poslati dvije preporuke koje nalikuju upozorenjima, a ako osoba nastavi s tim aktivnostima, dopis kojim se obavještava da te aktivnosti mogu predstavljati kaznena djela. Naposljetku, on ima pravo uputiti predmet državnom odvjetništvu radi kaznenog progona navedene osobe[66].

U tom kontekstu Državno vijeće traži od Suda da protumači Direktivu 2002/58, u vezi s Poveljom[67].

Kao prvo, kad je riječ o zadržavanju podataka o građanskom identitetu i odgovarajućim IP adresama, Sud naglašava da svako opće i neselektivno zadržavanje skupa IP adresa nužno ne predstavlja ozbiljno zadiranje u pravâ na poštovanje privatnosti, zaštitu osobnih podataka i slobodu izražavanja koja su zajamčena Poveljom.

Obveza osiguranja takvog zadržavanja može biti opravdana ciljem borbe protiv kaznenih djela općenito ako je stvarno isključeno da takvo zadržavanje može dovesti do ozbiljnih zadiranja u privatnost osobe o kojoj je riječ zbog mogućnosti donošenja konkretnih zaključaka o njoj, među ostalim, povezivanjem tih IP adresa sa skupom podataka o prometu ili o lokaciji.

Stoga se država članica koja namjerava pružateljima elektroničkih komunikacijskih usluga nametnuti takvu obvezu mora uvjeriti da načini zadržavanja tih podataka

---

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" (Uredba br. 2010-236 od 5. ožujka 2010. o automatskoj obradi osobnih podataka, koja je odobrena člankom L. 331-29 Zakonika o intelektualnom vlasništvu, pod nazivom „Sustav upravljanja mjerama za zaštitu djelâ na internetu" (JORF br. 56 od 7. ožujka 2010., tekst br. 19), kako je izmijenjen décretom 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 (Uredba br. 2017-924 od 6. svibnja 2017. o upravljanju tijela za ostvarivanje pravâ autorskim i srodnim pravima i o izmjeni Zakonika o intelektualnom vlasništvu) (JORF br. 109 od 10. svibnja 2017., tekst br. 176)

65 Osobito članak L. 331-21, treći, četvrti i peti stavak Zakonika o intelektualnom vlasništvu

66 Od 1. siječnja 2022. Hadopi je spojen s Conseilom supérieur de l'audiovisuel (Vrhovno vijeće za audiovizualne medije, u daljnjem tekstu: CSA), drugim neovisnim javnim tijelom, te oni sada zajedno čine Autorité de régulation de la communication audiovisuelle et numérique (Jedinstveno tijelo nadležno za audiovizualnu i digitalnu komunikaciju, u daljnjem tekstu: ARCOM). Postupak postupnog odgovora ipak se u bitnome nije promijenio.

67 Članak 15. stavak 1. Direktive 2002/58

isključuju mogućnost donošenja konkretnih zaključaka o privatnom životu osoba o kojima je riječ.

Sud pobliže određuje da se načini zadržavanja moraju, u tu svrhu, odnositi na samu strukturu zadržavanja koja u biti mora biti ustrojena na način da jamči stvarno nepropusno razdvajanje različitih kategorija zadržanih podataka. Stoga nacionalna pravila koja se odnose na te načine zadržavanja moraju osigurati da je svaka kategorija podataka, uključujući i podatke o građanskom identitetu i IP adresama, zadržana potpuno odvojeno od drugih kategorija zadržanih podataka i da je to zadržavanje stvarno nepropusno pomoću sigurnog i pouzdanog računalnog uređaja. Usto, u dijelu u kojem ta pravila predviđaju mogućnost povezivanja zadržanih IP adresa s građanskim identitetom osobe o kojoj je riječ radi borbe protiv kaznenih djela, ona smiju dopustiti takvo povezivanje samo upotrebom učinkovitog tehničkog postupka koji ne dovodi u pitanje učinkovitost nepropusnog razdvajanja tih kategorija podataka. Pouzdanost tog razdvajanja mora redovito nadzirati treće javno tijelo. Ako su u primjenjivom nacionalnom zakonodavstvu predviđeni takvi strogi zahtjevi, zadiranje koje proizlazi iz tog zadržavanja IP adresa ne može biti kvalificirano kao „ozbiljno”.

Stoga Sud zaključuje da se, ako postoji zakonsko uređenje koje jamči da se na temelju nijedne kombinacije podatka ne mogu donijeti konkretni zaključci o privatnom životu osoba čiji su podaci zadržani, Direktivi 2002/58, u vezi s Poveljom, ne protivi se to da država članica nametne obvezu općeg i neselektivnog zadržavanja IP adresa na razdoblje koje ne prekoračuje ono koje je strogo nužno radi postizanja cilja borbe protiv kaznenih djela općenito.

Kao drugo, što se tiče pristupa podacima o građanskom identitetu koji odgovaraju određenoj IP adresi, Sud presuđuje da se Direktivi 2002/58, u vezi s Poveljom, u načelu ne protivi nacionalni propis kojim se javnom tijelu dopušta pristup tim podacima koje su zasebno i stvarno nepropusno zadržali pružatelji elektroničkih komunikacijskih usluga, samo kako bi to tijelo moglo identificirati nositelje tih adresa osumnjičene da su počinili povrede autorskih i srodnih prava na internetu i kako bi moglo poduzeti mjere protiv njih. U takvom slučaju nacionalni propis mora službenicima koji imaju takav pristup zabraniti, prvo, da u bilo kojem obliku otkrivaju informacije o sadržaju datoteka kojima su pristupili ti nositelji, osim isključivo u svrhu upućivanja predmeta državnom odvjetništvu, drugo, da na bilo koji način prate tijek pretraživanja tih nositelja i, treće, da upotrebljavaju te IP adrese u svrhe različite od donošenja tih mjera.

U tom kontekstu Sud osobito podsjeća na to da, iako su sloboda izražavanja i povjerljivost osobnih podataka prioritet, ta temeljna prava ipak nisu apsolutna. Naime, u okviru odvagivanja prava i interesa o kojima je riječ oni se ponekad moraju povući pred drugim temeljnim pravima i razlozima u općem interesu, poput zaštite javnog poretka i sprečavanja kaznenih djela ili zaštite prava i sloboda drugih osoba. To je osobito tako kada prevaga navedenih prioriteta može narušiti učinkovitost kaznene istrage, među ostalim, onemogućujući ili pretjerano otežavajući učinkovitu identifikaciju počinitelja kaznenog djela i izricanje sankcije u odnosu na njega.

U istom tom kontekstu Sud također upućuje na svoju sudsku praksu, prema kojoj, kad je riječ o borbi protiv kaznenih djela kojima se povređuju autorska ili srodna prava počinjenih na internetu, okolnost da pristup IP adresama može biti jedino istražno sredstvo kojim se može identificirati osoba o kojoj je riječ pokazuje da su zadržavanje tih adresa i pristup njima strogo nužni za ostvarivanje cilja koji se nastoji postići i stoga ispunjavaju zahtjev proporcionalnosti. Nedopuštanje takvog pristupa bi, osim toga, dovelo do stvarne opasnosti od sustavnog nekažnjavanja kaznenih djela počinjenih na internetu čiji je počinjenje ili priprema olakšana samim značajkama interneta. Postojanje takve opasnosti predstavlja okolnost koja je relevantna za ocjenu, u okviru odvagivanja različitih postojećih prava i interesa, toga je li zadiranje u pravâ na poštovanje privatnosti, zaštitu osobnih podataka i slobodu izražavanja mjera koja je proporcionalna s obzirom na cilj borbe protiv kaznenih djela.

Kao treće, odlučujući o tome treba li pristup javnog tijela podacima o građanskom identitetu koji odgovaraju određenoj IP adresi podvrgnuti prethodnom nadzoru suda ili neovisnog upravnog tijela, Sud smatra da se zahtjev takvog nadzora nameće kada, u kontekstu nacionalnoga propisa, taj pristup podrazumijeva opasnost od ozbiljnog zadiranja u temeljna prava osobe o kojoj je riječ u smislu da bi on mogao omogućiti tom javnom tijelu da donese konkretne zaključke o privatnom životu te osobe i, ovisno o slučaju, da izradi njezin detaljan profil. Za razliku od toga, taj se zahtjev prethodnog nadzora ne primjenjuje kada se zadiranje u temeljna prava o kojima je riječ ne može kvalificirati kao ozbiljno.

S tim u vezi, Sud pojašnjava da, u slučaju u kojem se primjenjuje uređenje zadržavanja koje jamči stvarno nepropusno razdvajanje različitih kategorija zadržanih podataka, pristup javnog tijela podacima o građanskom identitetu koji odgovaraju tako zadržanim IP adresama u načelu nije podvrgnut zahtjevu prethodnog nadzora. Naime, takav pristup samo u svrhu identifikacije nositelja IP adrese u pravilu ne predstavlja ozbiljno zadiranje u navedena prava.

Međutim, Sud ne isključuje da u netipičnim situacijama postoji opasnost, u okviru postupka kao što je onaj postupnog odgovora o kojem je riječ u glavnom postupku, da javno tijelo može donijeti konkretne zaključke o privatnom životu osobe o kojoj je riječ, osobito kada se osoba bavi aktivnostima kojima se opetovano, pa i u velikoj mjeri, povređuju autorska ili srodna prava na P2P mrežama u vezi sa zaštićenim djelima posebnih vrsta koja mogu otkriti informacije koje, ovisno o slučaju, mogu biti osjetljive, o privatnosti te osobe.

U predmetnom slučaju nositelj određene IP adrese može biti osobito izložen takvoj opasnosti kada javno tijelo mora odlučiti o tome hoće li uputiti predmet državnom odvjetništvu radi kaznenog progona tog nositelja. Naime, intenzitet zadiranja u pravo na poštovanje privatnosti može se povećati kako postupak postupnog odgovora, koji se odvija u etapama, prolazi kroz svoje različite faze. Pristup nadležnog tijela svim podacima osobe o kojoj je riječ koji su prikupljeni tijekom različitih faza tog postupka može omogućiti da se donesu konkretni zaključci o njezinom privatnom životu. Slijedom

toga, nacionalni propis mora predvidjeti prethodni nadzor koji se mora provesti prije nego što javno tijelo može povezati podatke o građanskom identitetu i takav skup podataka i prije eventualnog slanja obavijesti kojom se utvrđuje da je ta osoba postupala na način koji može predstavljati kazneno djelo. Osim toga, taj nadzor mora očuvati učinkovitost postupka postupnog odgovora omogućujući osobito identifikaciju slučajeva mogućeg novog ponavljanja kažnjivog ponašanja o kojem je riječ. U tu svrhu taj postupak mora biti organiziran i strukturiran tako da podatke o građanskom identitetu osobe koji odgovaraju IP adresama koje su prethodno prikupljene na internetu osobe zadužene za ispitivanje činjenica u nadležnom javnom tijelu ne mogu automatski povezati s elementima kojima to tijelo već raspolaže i na temelju kojih se mogu donijeti konkretni zaključci o privatnom životu te osobe.

Usto, kad je riječ o predmetu prethodnog nadzora, Sud ističe da, u slučajevima u kojima je osoba o kojoj je riječ osumnjičena za počinjenje kaznenog djela koje je obuhvaćeno kaznenim djelima općenito, sud ili neovisno upravno tijelo zaduženo za taj nadzor mora uskratiti pristup kada on omogućuje javnom tijelu koje ga je zahtijevalo da donese konkretne zaključke o privatnom životu navedene osobe. Suprotno tomu, trebalo bi odobriti čak i pristup koji omogućuje donošenje takvih konkretnih zaključaka u slučaju u kojem se osoba o kojoj je riječ sumnjiči da je počinila kaznena djela za koja država članica o kojoj je riječ smatra da povređuju temeljni interes društva i stoga su obuhvaćena teškim oblicima kriminaliteta.

Sud isto tako pojašnjava da prethodni nadzor ni u kojem slučaju ne može biti u potpunosti automatiziran jer, kad je riječ o kaznenoj istrazi, takav nadzor zahtijeva odvagivanje, s jedne strane, legitimnih interesa povezanih s borbom protiv kriminaliteta i, s druge strane, poštovanja privatnosti i zaštite osobnih podataka. Takvo odvagivanje zahtijeva prisutnost fizičke osobe, koja je tim više potrebna kada automatizam i veliki opseg obrade podataka o kojima je riječ podrazumijevaju opasnost za privatnost.

Stoga Sud zaključuje da mogućnost da osobe zadužene za ispitivanje činjenica u okviru navedenog javnog tijela povezuju podatke o građanskom identitetu osobe koji odgovaraju određenoj IP adresi s datotekama koje sadržavaju elemente na temelju kojih je moguće saznati naslov zaštićenih djela čije je stavljanje na raspolaganje na internetu opravdalo to da organizacije nositeljâ prava prikupljaju IP adrese mora biti uvjetovana – u slučaju da ista osoba ponovi aktivnost kojom se povređuju autorska ili srodna prava – nadzorom suda ili neovisnog upravnog tijela. Taj nadzor ne može biti u potpunosti automatiziran i mora se provesti prije takvog povezivanja, koje u takvim slučajevima može omogućiti donošenje konkretnih zaključaka o privatnom životu navedene osobe čija je IP adresa upotrijebljena za aktivnosti kojima se mogu povrijediti autorska ili srodna prava.

Kao četvrto i posljednje, Sud navodi da sustav obrade podataka koji upotrebljava javno tijelo mora u pravilnim razmacima nadzirati neovisno tijelo koje ima svojstvo treće strane u odnosu na to javno tijelo. Cilj tog nadzora je provjera integriteta sustava, uključujući učinkovitih jamstava protiv opasnosti od zlouporabnog ili nezakonitog

pristupa i uporabe tih podataka, kao i njegove učinkovitosti i pouzdanosti za potrebe otkrivanja eventualnih povreda.

U okviru toga Sud primjećuje da u predmetnom slučaju prilikom automatizirane obrade osobnih podataka koju obavlja javno tijelo na temelju informacija o povredama koje su ustanovile organizacije nositeljâ prava može doći do određenog broja lažnih pozitivnih slučajeva kao i osobito opasnosti od toga da potencijalno visok broj osobnih podataka treće osobe zloupotrijebe ili nezakonito upotrijebe, što objašnjava nužnost takvog nadzora. Usto, on dodaje da takva obrada mora poštovati posebna pravila o zaštiti osobnih podataka koja su predviđena Direktivom 2016/680. Naime, u predmetnom slučaju, iako javno tijelo nema vlastite ovlasti odlučivanja u okviru postupka postupnog odgovora, ono se mora kvalificirati kao „javno tijelo" uključeno u sprečavanje i istragu kaznenih djela te je stoga obuhvaćeno područjem primjene te direktive. Stoga osobe obuhvaćene tim postupkom moraju imati pravo na sva materijalna i postupovna jamstva propisana Direktivom 2016/680, a zadaća je suda koji je uputio zahtjev da provjeri jesu li ona predviđena nacionalnim zakonodavstvom.

2. Obrada osobnih podataka u kaznenim stvarima

Presuda od 12. svibnja 2021. (veliko vijeće), Bundesrepublik Deutschland (Interpolova crvena tjeralica) (C-505/19, EU:C:2021:376*)*

Međunarodna organizacija kriminalističke policije (u daljnjem tekstu: Interpol) objavila je 2012. na zahtjev Sjedinjenih Američkih Država, na temelju uhidbenog naloga koji su izdala tijela te zemlje, crvenu tjeralicu za njemačkim državljaninom WS radi njegova mogućeg izručenja. Kada se u državi članici Interpola pronađe osoba koja je predmet takve tjeralice, ta država mora, u načelu, privremeno uhititi traženu osobu, nadzirati je ili ograničiti njezino kretanje.

Međutim, čak i prije objave te crvene tjeralice, u Njemačkoj je protiv osobe WS pokrenut istražni postupak koji se, prema mišljenju suda koji je uputio zahtjev, odnosio na ista djela kao što su to ona na kojima se temelji ta tjeralica. Taj je postupak pravomoćno zaključen 2010. nakon što je osoba WS platila novčani iznos u skladu s posebnim postupkom sporazumijevanja o kazni, koji je predviđen njemačkim kaznenim pravom. Nakon toga je Bundeskriminalamt (Savezni ured kriminalističke policije, Njemačka) obavijestio Interpol da smatra da je zbog tog ranijeg postupka u ovom slučaju primjenjivo načelo *ne bis in idem*. Tim se načelom, koje je sadržano u članku 54. Konvencije o provedbi Schengenskog sporazuma[68] i članku 50. Povelje, zabranjuje, među

[68] Konvencija o provedbi Schengenskog sporazuma od 14. lipnja 1985. između vlada država Gospodarske unije Beneluksa, Savezne Republike Njemačke i Francuske Republike o postupnom ukidanju kontrola na zajedničkim granicama (SL 2000., L 239, str. 19.) (SL, posebno izdanje na hrvatskom jeziku, poglavlje 19., svezak 9., str. 12. i ispravak SL 2018., L 41, str. 15.; u daljnjem tekstu: CISA)

ostalim, da se protiv osobe protiv koje je sudski postupak već pravomoćno okončan vodi novi kazneni postupak za isto kazneno djelo.

Osoba WS podnijela je 2017. Verwaltungsgerichtu Wiesbaden (Upravni sud u Wiesbadenu, Njemačka) tužbu protiv Savezne Republike Njemačke kako bi joj se naložilo poduzimanje potrebnih mjera za povlačenje te crvene tjeralice. U tom pogledu osoba WS ističe povredu načela *ne bis in idem* i povredu svojeg prava na slobodno kretanje, zajamčenog člankom 21. UFEU-a, s obzirom na to da ne može otići u državu stranku Schengenskog sporazuma ili u državu članicu a da se pritom ne dovede u opasnost od uhićenja. Također smatra da je zbog tih povreda obrada njezinih osobnih podataka iz crvene tjeralice protivna Direktivi 2016/680 o zaštiti osobnih podataka u kaznenim stvarima[69].

U tom je kontekstu Upravni sud u Wiesbadenu odlučio uputiti Sudu pitanja o primjeni načela *ne bis in idem* i, konkretnije, o mogućnosti privremenog uhićenja osobe koja je predmet crvene tjeralice u situaciji poput one o kojoj je riječ. Usto, u slučaju primjenjivosti tog načela, taj sud želi znati posljedice u pogledu obrade osobnih podataka sadržanih u takvoj tjeralici koju provode države članice.

U svojoj presudi Sud, u sastavu velikog vijeća, presuđuje da odredbe Direktive 2016/680, u vezi s člankom 54. CISA-e i člankom 50. Povelje, treba tumačiti na način da im se ne protivi obrada osobnih podataka iz crvene tjeralice koju je izdao Interpol ako takvom sudskom odlukom nije utvrđeno da se na djela na kojima se temelji ta tjeralica primjenjuje načelo *ne bis in idem*, pod uvjetom da takva obrada ispunjava uvjete predviđene tom direktivom.

Kad je riječ o pitanju u pogledu osobnih podataka iz Interpolove crvene tjeralice, Sud navodi da svaki postupak koji se primjenjuje na te podatke, poput njihova bilježenja u popise tjeralica države članice, predstavlja „obradu” koja je obuhvaćena Direktivom 2016/680[70]. Usto, on smatra, s jedne strane, da se tom obradom ostvaruje zakonita svrha i, s druge strane, da se ta obrada ne može smatrati nezakonitom samo zato što bi se načelo *ne bis in idem* moglo primijeniti na djela na kojima se temelji crvena tjeralica[71]. Uostalom, ta se obrada koju provode tijela država članica može pokazati nužnom upravo u svrhu provjere primjenjuje li se navedeno načelo.

U tim okolnostima Sud također smatra da se Direktivi 2016/680, u vezi s člankom 54. CISA-e i člankom 50. Povelje, ne protivi obrada osobnih podataka iz crvene tjeralice ako pravomoćnom sudskom odlukom nije utvrđeno da se u konkretnom slučaju primjenjuje načelo *ne bis in idem*. Međutim, takva obrada mora poštovati uvjete predviđene tom direktivom. U tom smislu obrada mora biti, među ostalim, nužna kako bi nadležno

[69] Direktiva (EU) 2016/680 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka od strane nadležnih tijela u svrhe sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Okvirne odluke Vijeća 2008/977/PUP (SL 2016., L 119, str. 89. i ispravak SL 2018., L 127, str. 14.)

[70] Vidjeti članak 2. stavak 1. i članak 3. točku 2. Direktive 2016/680.

[71] Vidjeti članak 4. stavak 1. točku (b) i članak 8. stavak 1. Direktive 2016/680.

nacionalno tijelo obavilo zadaću u svrhe sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija[72].

Nasuprot tomu, kad se primjenjuje načelo *ne bis in idem*, bilježenje osobnih podataka iz Interpolove crvene tjeralice u popise tjeralica država članica više nije nužno jer se protiv predmetne osobe više ne može voditi kazneni postupak za djela obuhvaćena navedenom tjeralicom i, slijedom toga, ne može je se zbog njih uhititi. Iz toga slijedi da ispitanik mora imati mogućnost zatražiti brisanje svojih podataka. Ako se to bilježenje ipak zadržava, ono mora biti popraćeno navodom da se zbog načela *ne bis in idem* protiv predmetne osobe više ne može voditi kazneni postupak u državi članici odnosno državi ugovornici za ista djela.

Presuda od 21. lipnja 2022. (veliko vijeće), Ligue des droits humains (C-817/19, EU:C:2022:491)

U tom predmetu (vidjeti također poglavlje I.1., naslovljeno „Usklađenost sekundarnog prava Unije s pravom na zaštitu osobnih podataka”), nakon što je utvrdio valjanost Direktive o PNR-u, Sud daje pojašnjenja u pogledu nekih njezinih odredbi[73].

Kao prvo, ističe da se u Direktivi iscrpno navode ciljevi koji se nastoje postići obradom podataka iz PNR-a. Slijedom toga, toj se direktivi protivi nacionalno zakonodavstvo kojim se dopušta obrada podataka iz PNR-a u svrhe koje se razlikuju od borbe protiv kaznenih djela terorizma i teških kaznenih djela. Prema tome, nacionalno zakonodavstvo kojim se usto kao svrha obrade podataka iz PNR-a priznaje praćenje aktivnosti obavještajnih i sigurnosnih službi može povrijediti iscrpnost tog navođenja. Isto tako, sustav uspostavljen Direktivom o PNR-u ne može se predvidjeti u svrhu poboljšanja graničnih kontrola i sprečavanja ilegalne migracije. Iz toga slijedi i da se podaci iz PNR-a ne mogu čuvati u jedinstvenoj bazi podataka kojoj se može pristupiti radi postizanja svrha iz Direktive o PNR-u i drugih svrha.

Kao drugo, Sud objašnjava pojam neovisnog nacionalnog tijela, koje je nadležno za provjeru toga jesu li ispunjeni uvjeti za dostavu podataka iz PNR-a u svrhu njihove naknadne procjene te za odobravanje takve dostave. Konkretno, tijelo uspostavljeno kao PIU ne može se kvalificirati kao takvo neovisno nacionalno tijelo jer nema svojstvo treće strane u odnosu na tijelo koje traži pristup podacima. Naime, budući da članovi njegova osoblja mogu biti službenici koje su ovlaštena tijela uputila da zatraže takav pristup, PIU je nužno povezan s tim tijelima. Stoga se Direktivi o PNR-u protivi nacionalno zakonodavstvo u skladu s kojim tijelo uspostavljeno kao PIU također ima svojstvo nadležnog nacionalnog tijela koje je ovlašteno dopustiti otkrivanje podataka iz PNR-a nakon isteka razdoblja od šest mjeseci nakon prijenosa tih podataka PIU-u.

[72] Vidjeti članak 1. stavak 1. i članak 8. stavak 1. Direktive 2016/680.

[73] Konkretno, članka 2. („Primjena [...] Direktive na letove unutar EU-a”), članka 6. („Obrada podataka iz PNR-a”) i članka 12. („Razdoblje čuvanja i depersonalizacije podataka”) Direktive o PNR-u

Kao treće, što se tiče roka za čuvanje podataka iz PNR-a, Sud odlučuje da se članku 12. Direktive o PNR-u, u vezi s člancima 7. i 8. te člankom 52. stavkom 1. Povelje, protivi nacionalno zakonodavstvo kojim se za čuvanje tih podataka predviđa opći rok od pet godina, koji se bez razlike primjenjuje na sve zrakoplovne putnike.

Naime, prema mišljenju Suda, nakon isteka početnog razdoblja za čuvanje od šest mjeseci, čuvanje podataka iz PNR-a nije ograničeno na ono što je strogo nužno kad je riječ o zrakoplovnim putnicima u pogledu kojih ni prethodna procjena ni eventualne provjere provedene tijekom početnog razdoblja čuvanja od šest mjeseci ni bilo koja druga okolnost nisu otkrile postojanje objektivnih elemenata, kao što je činjenica da su podaci iz PNR-a o dotičnim putnicima doveli do pozitivnog rezultata provjerenog u okviru prethodne procjene, na temelju kojih se može utvrditi opasnost u pogledu kaznenih djela terorizma ili teških kaznenih djela koja su, makar i posredno, objektivno povezana sa zračnim prijevozom tih putnika. Suprotno tomu, smatra da tijekom početnog razdoblja od šest mjeseci čuvanje podataka iz PNR-a o svim zrakoplovnim putnicima koje je obuhvaćeno sustavom uspostavljenim tom direktivom u načelu ne prekoračuje granice onoga što je strogo nužno.

Kao četvrto, Sud pruža smjernice u pogledu eventualne primjene Direktive o PNR-u, u svrhu borbe protiv kaznenih djela terorizma i teških kaznenih djela, na druga prijevozna sredstva kojima se putnici prevoze u Uniji. Međutim, Direktivi se, u vezi s člankom 3. stavkom 2. UEU-a, člankom 67. stavkom 2. UFEU-a i člankom 45. Povelje, protivi sustav prijenosa i obrade podataka iz PNR-a o svim prijevozima koji se odvijaju drugim sredstvima unutar Unije ako se dotična država članica ne suočava sa stvarnom i trenutačnom ili predvidljivom terorističkom prijetnjom. U takvoj situaciji, kao i za letove unutar EU-a, primjenu sustava uspostavljenog Direktivom o PNR-u treba ograničiti na podatke iz PNR-a o prijevozima koji se osobito odnose na određene linije ili obrasce putovanja ili pak određene kolodvore ili morske luke za koje postoje naznake koje mogu opravdati tu primjenu. Na dotičnoj je državi članici da odabere prijevoze za koje postoje takve naznake i da redovito preispituje tu primjenu s obzirom na promjenu uvjeta koji opravdavaju njezin odabir.

IV. Prijenos osobnih podataka trećim zemljama

Presuda od 6. studenoga 2003. (veliko vijeće), Lindqvist (C-101/01, EU:C:2003:596)

U tom je predmetu (vidjeti također poglavlje II.3., naslovljeno „Pojam ‚obrada osobnih podataka’”) sud koji je uputio zahtjev želio doznati, među ostalim, je li B. Lindqvist prenosila podatke trećim zemljama u smislu navedene direktive.

Sud presuđuje da ne postoji „prijenos podataka trećim zemljama” u smislu članka 25. Direktive 95/46 kada osoba koja se nalazi u državi članici upisuje osobne podatke na internetsku stranicu pohranjenu kod fizičke ili pravne osobe koja poslužuje internetsko mjesto gdje se može posjetiti ta stranica i koja ima prebivalište odnosno poslovni nastan u toj ili drugoj državi članici, čineći ih na taj način dostupnima svakoj osobi koja se spoji na internet, uključujući osobe koje se nalaze u trećim zemljama.

Naime, imajući u vidu, s jedne strane, stanje razvoja interneta u vrijeme izrade Direktive 95/46 i, s druge strane, nepostojanje kriterija primjenjivih na uporabu interneta u njezinu poglavlju IV., koje obuhvaća taj članak 25. – kojim se nastoji osigurati nadzor država članica nad prijenosom osobnih podataka trećim zemljama i zabrana takvih prijenosa ako ne pružaju odgovarajuću razinu zaštite – ne može se pretpostaviti da je zakonodavac Zajednice namjeravao uključiti *pro futuro* u pojam „prijenos podataka trećim zemljama” takav upis podataka na internetsku stranicu, čak i ako su na taj način dostupni osobama iz trećih zemalja koje imaju tehnička sredstva da im pristupe.

Presuda od 6. listopada 2015. (veliko vijeće), Schrems (C-362/14, EU:C:2015:650)

M. Schrems, austrijski državljanin i korisnik društvene mreže Facebook, uputio je pritužbu Data Protection Commissioneru (povjerenik za zaštitu podataka, Irska) jer je društvo Facebook Ireland prenosilo u Sjedinjene Američke Države osobne podatke svojih korisnika te ih je pohranjivalo na svojim poslužiteljima smještenima na državnom području SAD-a, gdje su bili predmet obrade. Prema Schremsovim tvrdnjama, pravo i praksa u SAD-u nisu nudili dovoljnu razinu zaštite od nadzora javnih tijela osobnih podataka prenesenih toj zemlji. Povjerenik za zaštitu podataka odbio je pritužbu, među ostalim, zato što je Komisija u svojoj Odluci 2000/520/EZ[74] smatrala da SAD u okviru sustava „sigurne luke” (eng. *safe harbour*)[75] osigurava odgovarajuću razinu zaštite prenesenih osobnih podataka.

U tom je kontekstu High Court (Visoki sud, Irska) podnio Sudu zahtjev za tumačenje članka 25. stavka 6. Direktive 95/46, na temelju kojeg je Komisija mogla utvrditi da treća zemlja osigurava odgovarajuću razinu zaštite prenesenih podataka, kao i zahtjev za meritorno utvrđivanje valjanosti Odluke Komisije 2000/520, donesene na temelju navedenog članka 25. stavka 6. Direktive 95/46.

Sud Komisijinu odluku proglašava nevaljanom u cijelosti, naglašavajući, prije svega, da je njezino donošenje zahtijevalo valjano Komisijino obrazloženo utvrđenje da dotična treća zemlja djelotvorno osigurava razinu zaštite temeljnih prava koja je bitno jednakovrijedna onoj koja se jamči u pravnom poretku Unije. Međutim, s obzirom na to da Komisija u svojoj Odluci 2000/520 to nije učinila, njezinim člankom 1. povrijeđeni su zahtjevi utvrđeni u članku 25. stavku 6. Direktive 95/46 u vezi s Poveljom te je stoga taj članak 1.

[74] Odluka Komisije 2000/520/EZ od 26. srpnja 2000. sukladno s Direktivom 95/46/EZ Europskog parlamenta i Vijeća o primjerenosti zaštite koju pružaju načela privatnosti „sigurne luke” i uz njih vezana često postavljana pitanja koje je izdalo Ministarstvo trgovine SAD-a (SL 2000., L 215, str. 7.) (SL, posebno izdanje na hrvatskom jeziku, poglavlje 16., svezak 3., str. 9.)

[75] Sustav „sigurne luke” obuhvaća niz načela o zaštiti osobnih podataka kojima poduzeća iz SAD-a mogu dobrovoljno pristupiti.

nevaljan. Naime, načela „sigurne luke” primjenjuju se jedino na organizacije iz SAD-a koje su provele vlastito potvrđivanje i primaju osobne podatke iz Unije, a javna tijela SAD-a nisu podvrgnuta poštovanju navedenih načela. Štoviše, Odlukom 2000/520 omogućuje se zadiranje u temeljna prava osoba čiji se osobni podaci prenose ili bi se mogli prenositi iz Unije u SAD a da ne sadržava nikakvo utvrđenje o postojanju državnih pravila SAD-a za ograničavanje mogućih zadiranja u ta prava kao ni utvrđenje o učinkovitoj pravnoj zaštiti protiv takvih zadiranja.

Usto, Sud proglašava nevaljanim članak 3. Odluke 2000/520 jer se njime nacionalnim nadzornim tijelima oduzimaju ovlasti koje ona imaju na temelju članka 28. Direktive 95/46 u slučaju kada osoba navede elemente koji mogu dovesti u pitanje usklađenost Komisijine odluke kojom je utvrđeno da treća zemlja osigurava odgovarajuću razinu zaštite sa zaštitom privatnog života i temeljnih sloboda i prava pojedinaca. Sud zaključuje da je nevaljanost članaka 1. i 3. Odluke 2000/520 utjecala na valjanost te odluke u cijelosti.

Kad je riječ o nemogućnosti opravdanja takvog zadiranja, Sud ponajprije navodi da propis Unije koji zadire u temeljna prava zajamčena u člancima 7. i 8. Povelje mora predvidjeti jasna i precizna pravila koja uređuju doseg i primjenu mjere te propisati minimalne uvjete na način da ispitanici raspolažu dostatnim jamstvima koja omogućuju učinkovitu zaštitu njihovih podataka od opasnosti zlouporabe kao i od svih nezakonitih pristupa i uporaba tih podataka. Nužnost raspolaganja takvim jamstvima još je i važnija kada su osobni podaci podvrgnuti automatskoj obradi te postoji znatna opasnost od nezakonitog pristupa tim podacima.

Osim toga i iznad svega, zaštita temeljnog prava na poštovanje privatnog života na razini Unije zahtijeva da su odstupanja i ograničenja u zaštiti osobnih podataka u granicama onoga što je krajnje nužno. Stoga propis koji općenito dopušta zadržavanje cjelokupnih osobnih podataka svih osoba čiji su podaci preneseni iz Unije, bez ikakva razlikovanja, ograničenja ili iznimke s obzirom na zadani cilj, i koji ne predviđa objektivan kriterij koji bi omogućavao ograničenje pristupa javnih tijela podacima i njihovu naknadnu uporabu u svrhe koje su točno određene, usko ograničene i mogu opravdati zadiranje koje obuhvaća i pristup i uporabu tih podataka nije ograničen na ono što je krajnje nužno. Posebice, nužno je smatrati da propis koji omogućava javnim tijelima općenit pristup sadržaju elektroničkih komunikacija povređuje bitan sadržaj temeljnog prava na poštovanje privatnog života. Također, propis koji pojedincima ne pruža nikakvu mogućnost korištenja pravnim sredstvima radi pristupa osobnim podacima koji se na njih odnose, ili radi ispravka ili brisanja takvih podataka, ne poštuje bitan sadržaj temeljnog prava na djelotvornu sudsku zaštitu, kao što je to propisano u članku 47. Povelje.

Mišljenje 1/15 (Sporazum o PNR-u EU-Kanada) od 26. srpnja 2017. (veliko vijeće) (EU:C:2017:592)

Sud je 26. srpnja 2017. prvi put odlučivao o usklađenosti prijedloga međunarodnog sporazuma s Poveljom, a osobito s odredbama o poštovanju privatnog života i zaštiti osobnih podataka.

Europska unija i Kanada ispregovarali su sporazum o prijenosu i obradi podataka iz evidencije podataka o putnicima (sporazum o PNR-u), koji je potpisan 2014. Budući da je Vijeće Europske unije od Europskog parlamenta zatražilo suglasnost za Prijedlog odluke Vijeća o sklapanju predviđenog sporazuma, Europski parlament odlučio je pokrenuti postupak pred Sudom radi davanja mišljenja o usklađenosti predviđenog sporazuma s pravom Unije.

Predviđeni sporazum omogućava sustavan i kontinuiran prijenos podataka iz PNR-a svih putnika u zračnom prometu kanadskom tijelu radi njihova korištenja i čuvanja te eventualnog daljnjeg prenošenja drugim tijelima i ostalim trećim zemljama u cilju borbe protiv terorizma i teških oblika prekograničnog kriminaliteta. U tu je svrhu predviđenim sporazumom propisano, među ostalim, petogodišnje čuvanje podataka, utvrđeni su posebni zahtjevi u pogledu sigurnosti i integriteta podataka iz PNR-a, kao što je to trenutačno prikrivanje osjetljivih podataka, te su propisana prava pristupa, ispravka i brisanja podataka kao i mogućnost podnošenja upravnih i sudskih pravnih sredstava.

Podaci iz PNR-a na koje se odnosi predviđeni sporazum obuhvaćaju, među ostalim, ime i kontaktne podatke putnika u zračnom prometu, informacije potrebne za rezervaciju, kao što su to datumi planiranog putovanja i plan putovanja, informacije o kartama, skupinama osoba registriranih pod istim brojem rezervacije, informacije o načinu plaćanja ili o izdavanju računa, informacije o prtljazi te opće primjedbe u pogledu putnika.

Sud u mišljenju smatra da se sporazum o PNR-u ne može zaključiti u postojećem obliku zbog neusklađenosti većeg broja njegovih odredbi s temeljnim pravima koje priznaje Unija.

Sud utvrđuje, kao prvo, da prijenos podataka iz PNR-a iz Unije prema nadležnom kanadskom tijelu i okvir koji je Unija dogovorila s Kanadom u pogledu uvjeta čuvanja tih podataka, njihova korištenja i eventualnog daljnjeg prenošenja drugim kanadskim tijelima, Europolu, Eurojustu, pravosudnim ili policijskim tijelima država članica ili pak tijelima ostalih trećih zemalja predstavljaju zadiranja u pravo zajamčeno člankom 7. Povelje. Tim se radnjama također zadire u temeljno pravo na zaštitu osobnih podataka zajamčeno u članku 8. Povelje, s obzirom na to da se njima obrađuju osobni podaci.

Usto, Sud naglašava da, iako se ne čini da bi pojedini podaci iz PNR-a, promatrani izdvojeno, mogli otkrivati važne informacije o privatnom životu ispitanika, oni ipak mogu u cjelini, među ostalim, otkrivati cjelokupan plan putovanja, putne navike, odnose između dviju ili više osoba kao i informacije o financijskim prilikama putnika u zračnom prometu, njihovim prehrambenim navikama ili zdravstvenom stanju te čak mogu pružati

osjetljive informacije o tim putnicima, kako su definirane u članku 2. točki (e) predviđenog sporazuma (informacije o rasnom ili etničkom podrijetlu, političkim gledištima, vjerskim uvjerenjima itd.).

U tom pogledu Sud smatra da, iako se predmetno zadiranje može opravdati ciljem od općeg interesa (osiguravanje javne sigurnosti u okviru borbe protiv kaznenih djela terorizma i teških oblika prekograničnog kriminaliteta), mnoge odredbe sporazuma nisu ograničene na ono što je krajnje nužno te ne propisuju jasna i precizna pravila.

Sud osobito navodi da bi, uzimajući u obzir opasnost od obrade protivne načelu nediskriminacije, prijenos osjetljivih podataka Kanadi zahtijevao precizno i veoma čvrsto opravdanje koje se temelji na drugim razlozima osim zaštite javne sigurnosti od terorizma i teških oblika prekograničnog kriminaliteta. Međutim, u konkretnom slučaju takvo opravdanje ne postoji. Sud zaključuje da su odredbe sporazuma o prijenosu osjetljivih podataka Kanadi te njihova obrada i čuvanje neusklađeni s temeljnim pravima.

Kao drugo, Sud smatra da produljeno pohranjivanje podataka iz PNR-a svih putnika u zračnom prometu nakon njihova odlaska iz Kanade, koje je dopušteno predviđenim sporazumom, nije ograničeno na ono što je krajnje nužno. Naime, kad je riječ o putnicima u zračnom prometu u pogledu kojih prilikom njihova dolaska u Kanadu i sve do njihova odlaska iz te treće zemlje nije bila utvrđena opasnost u području terorizma ili teških oblika prekograničnog kriminaliteta, nije izgledno da nakon njihova odlaska postoji veza, makar i neizravna, između njihovih podataka iz PNR-a i cilja zadanog predviđenim sporazumom koja bi opravdavala čuvanje tih podataka. Nasuprot tomu, pohranjivanje podataka iz PNR-a putnika u zračnom prometu za koje je utvrđeno postojanje objektivnih elemenata iz kojih se može zaključiti da bi čak i nakon njihova odlaska iz Kanade mogli predstavljati opasnost u kontekstu borbe protiv terorizma i teških oblika prekograničnog kriminaliteta dopušteno je i izvan okvira njihova boravka u Kanadi, čak u trajanju od pet godina.

Kao treće, Sud utvrđuje da temeljno pravo na poštovanje privatnog života, sadržano u članku 7. Povelje, podrazumijeva da se ispitanik može uvjeriti da se njegovi osobni podaci obrađuju pravilno i zakonito. Kako bi mogao obaviti nužne provjere, taj ispitanik mora raspolagati pravom na pristup podacima koji se na njega odnose, a predmet su obrade.

U tom pogledu Sud naglašava da putnici u zračnom prometu prema predviđenom sporazumu moraju biti informirani o prijenosu svojih podataka iz PNR-a u dotičnu treću zemlju i o korištenju tih podataka od trenutka kad to priopćavanje ne može ugroziti istrage koje provode javna tijela određena predviđenim sporazumom. Naime, takva je informacija zapravo potrebna da bi se putnicima u zračnom prometu omogućilo korištenje njihovim pravima na zahtijevanje pristupa podacima koji se na njih odnose i, eventualno, njihovo ispravljanje, kao i na djelotvoran pravni lijek pred sudom u skladu s člankom 47. prvim stavkom Povelje.

Dakle, pojedinačno obavještavanje putnika u zračnom prometu nužno je u slučajevima kad postoje objektivni elementi koji opravdavaju korištenje podataka iz PNR-a radi borbe

protiv terorizma i teških oblika prekograničnog kriminaliteta i zahtijevaju prethodno odobrenje pravosudnog ili neovisnog upravnog tijela. Isto vrijedi i u slučaju kad se podaci iz PNR-a zrakoplovnih putnika dostavljaju drugim javnim tijelima ili privatnim subjektima. Međutim, takvo se informiranje mora provesti tek u trenutku kad ono ne može ugroziti istrage koje provode javna tijela određena predviđenim sporazumom.

Presuda od 16. srpnja 2020. (veliko vijeće), Facebook Ireland i Schrems (C-311/18, EU:C:2020:559)

OUZP-om se određuje da do prijenosa podataka trećoj zemlji u pravilu može doći samo ako predmetna treća zemlja osigurava primjerenu razinu zaštite tih podataka. U skladu s tom uredbom, Komisija može utvrditi da treća zemlja na temelju domaćeg zakonodavstva ili međunarodnih obveza koje je preuzela osigurava primjerenu razinu zaštite[76]. Ako ne postoji takva odluka o primjerenosti, takav prijenos može se izvršiti samo ako izvoznik osobnih podataka s poslovnim nastanom u Uniji predvidi odgovarajuće zaštitne mjere koje se mogu temeljiti osobito na standardnim klauzulama o zaštiti podataka koje je donijela Komisija i pod uvjetom da su osobama na koje se podaci odnose na raspolaganju provediva prava i djelotvorni pravni lijekovi[77]. Nadalje, OUZP-om se precizno utvrđuju uvjeti pod kojima može doći do takvog prijenosa kad ne postoje odluka o primjerenosti ili odgovarajuće zaštitne mjere[78].

Maximillian Schrems, austrijski državljanin s boravištem u Austriji, korisnik je Facebooka od 2008. Kao i u slučaju drugih korisnika s boravištem u Uniji, osobne podatke M. Schremsa Facebook Ireland u cijelosti ili djelomično prenosi na poslužitelje koji pripadaju društvu Facebook Inc. i koji su smješteni na državnom području Sjedinjenih Američkih Država, gdje su predmet obrade. M. Schrems irskom nadzornom tijelu podnio je pritužbu kojom je u biti zatražio zabranu tih prijenosa. Tvrdio je da pravo i prakse u SAD-u ne jamče dovoljnu razinu zaštite od pristupa javnih tijela podacima prenesenima u tu zemlju. Ta je pritužba odbijena, među ostalim, zbog toga što je Komisija u svojoj Odluci 2000/520[79] utvrdila da SAD osigurava primjerenu razinu zaštite. Presudom donesenom 6. listopada 2015. Sud je, odlučujući o prethodnom pitanju koje je uputio High Court (Visoki sud, Irska), tu odluku proglasio nevaljanom (u daljnjem tekstu: presuda Schrems I)[80].

Nakon presude Schrems I i nakon što je irski sud naknadno poništio odluku o odbijanju pritužbe M. Schremsa, irsko nadzorno tijelo pozvalo je M. Schremsa da preformulira svoju pritužbu, s obzirom na to da je Sud poništio Odluku 2000/520. U svojoj preformuliranoj pritužbi M. Schrems i dalje je tvrdio da SAD ne nudi dovoljnu zaštitu podataka prenesenih u tu zemlju. On je tražio da se ubuduće obustave ili zabrane

[76] Članak 45. OUZP-a

[77] Članak 46. stavak 1. i članak 46. stavak 2. točka (c) OUZP-a

[78] Članak 49. OUZP-a

[79] Odluka Komisije od 26. srpnja 2000. sukladno s Direktivom 95/46/EZ Europskog parlamenta i Vijeća o primjerenosti zaštite koju pružaju načela privatnosti „sigurne luke" i uz njih vezana često postavljana pitanja koje je izdalo Ministarstvo trgovine SAD-a (SL 2000., L 215, str. 7.) (SL, posebno izdanje na hrvatskom jeziku, poglavlje 16., svezak 3., str. 9.)

[80] Presuda Suda od 6. listopada 2015., Schrems, C-362/14, EU:C:2015:650

prijenosi njegovih osobnih podataka iz Unije u SAD, koje Facebook Ireland sada izvršava na temelju standardnih klauzula o zaštiti koje se nalaze u Prilogu Odluci 2010/87[81]. Smatrajući da odlučivanje o pritužbi M. Schremsa ovisi osobito o valjanosti Odluke 2010/87, irsko nadzorno tijelo pokrenulo je postupak pred High Courtom (Visoki sud) kako bi on uputio Sudu zahtjev za prethodnu odluku. Nakon pokretanja tog postupka, Komisija je donijela Odluku (EU) 2016/1250 o primjerenosti zaštite u okviru europsko-američkog sustava zaštite privatnosti[82].

Svojim zahtjevom za prethodnu odluku sud koji je uputio zahtjev pitao je Sud o primjenjivosti OUZP-a na prijenose osobnih podataka koji se temelje na standardnim klauzulama o zaštiti iz Odluke 2010/87, o razini zaštite koja se zahtijeva tom uredbom u okviru takvog prijenosa i o obvezama nadzornih tijela u tom kontekstu. Nadalje, High Court (Visoki sud) pitao se o valjanosti kako Odluke 2010/87 tako i Odluke 2016/1250.

Sud utvrđuje da ispitivanje Odluke 2010/87 s obzirom na Povelju ne otkriva nijedan element koji bi mogao utjecati na njezinu valjanost. Nasuprot tomu, Odluku 2016/1250 proglašava nevaljanom.

Kao prvo, Sud smatra da se pravo Unije, među ostalim OUZP, primjenjuje na osobne podatke koje u komercijalne svrhe gospodarski subjekt s poslovnim nastanom u državi članici prenosi na drugi gospodarski subjekt s poslovnim nastanom u trećoj zemlji, čak i ako bi tijekom ili nakon tog prijenosa te podatke mogla obrađivati tijela predmetne treće zemlje za potrebe javne sigurnosti, obrane ili nacionalne sigurnosti. On pojašnjava da ta vrsta obrade podataka tijela treće zemlje ne može takav prijenos isključiti iz područja primjene OUZP-a.

Kad je riječ o razini zaštite koja se zahtijeva u okviru takvog prijenosa, Sud presuđuje da se zahtjevi koji su u tu svrhu predviđeni odredbama OUZP-a, koji se odnose na odgovarajuće zaštitne mjere, provediva prava i djelotvorne pravne lijekove, moraju tumačiti na način da osobe čiji se osobni podaci prenose u treću zemlju na temelju standardnih klauzula o zaštiti podataka moraju imati pravo na razinu zaštite koja je bitno ekvivalentna onoj zajamčenoj u Uniji tom uredbom, tumačenom u vezi s Poveljom. U tom kontekstu Sud pojašnjava da se pri ocjeni te razine zaštite moraju uzeti u obzir kako ugovorne odredbe koje su ugovorili izvoznik podataka s poslovnim nastanom u Uniji i primatelj podataka s poslovnim nastanom u predmetnoj trećoj zemlji tako i, kad je riječ o eventualnom pristupu javnih tijela te treće zemlje tako prenesenim podacima, relevantni elementi njezina pravnog sustava.

Kad je riječ o obvezama nadzornih tijela u kontekstu takvog prijenosa, Sud presuđuje da su, osim ako postoji odluka o primjerenosti koju je Komisija valjano donijela, ta tijela osobito dužna obustaviti ili zabraniti prijenos osobnih podataka u treću zemlju kada

[81] Odluka Komisije od 5. veljače 2010. o standardnim ugovornim klauzulama za prijenos osobnih podataka obrađivačima u trećim zemljama u skladu s Direktivom 95/46/EZ Europskog parlamenta i Vijeća (SL 2010., L 39, str. 5.) (SL, posebno izdanje na hrvatskom jeziku, poglavlje 13., svezak 52., str. 250.), kako je izmijenjena Provedbenom odlukom Komisije (EU) 2016/2297 od 16. prosinca 2016. (SL 2016., L 344, str. 100.)

[82] Provedbena odluka Komisije (EU) 2016/1250 od 12. srpnja 2016. o primjerenosti zaštite u okviru europsko-američkog sustava zaštite privatnosti u skladu s Direktivom 95/46/EZ Europskog parlamenta i Vijeća (SL 2016., L 207, str. 1.)

smatraju, u vezi sa svim okolnostima tog prijenosa, da standardne klauzule o zaštiti podataka nisu ili ne mogu biti poštovane u toj zemlji i da se zaštita prenesenih podataka koja se zahtijeva pravom Unije ne može osigurati drugim sredstvima, ako izvoznik s poslovnim nastanom u Uniji sam nije obustavio takav prijenos ili ga okončao.

Sud potom razmatra valjanost Odluke 2010/87. Sud smatra da njezina valjanost nije dovedena u pitanje samom činjenicom da standardne klauzule o zaštiti podataka koje se u njoj nalaze zbog svoje ugovorne naravi ne obvezuju tijela treće zemlje u koju bi se mogli prenijeti podaci. Nasuprot tomu, on pojašnjava da ta valjanost ovisi o tome sadržava li navedena odluka učinkovite mehanizme koji u praksi omogućuju osiguranje razine zaštite koja se zahtijeva pravom Unije i obustavu ili zabranu prijenosa osobnih podataka temeljenih na takvim klauzulama, u slučaju povrede tih klauzula ili nemogućnosti njihova poštovanja. Sud utvrđuje da se Odlukom 2010/87 uspostavljaju takvi mehanizmi. U tom pogledu on osobito ističe da je tom odlukom uvedena obveza izvoznika podataka i njihova primatelja da prethodno provjere poštuje li predmetna treća zemlja tu razinu zaštite te ta odluka obvezuje tog primatelja da obavijesti izvoznika podataka o svojoj eventualnoj nemogućnosti da postupi u skladu sa standardnim klauzulama o zaštiti, a na potonjem je da obustavi prijenos podataka i/ili raskine ugovor sklopljen s primateljem.

Sud naposljetku razmatra valjanost Odluke 2016/1250 u pogledu zahtjeva koji proizlaze iz OUZP-a, tumačenog u vezi s odredbama Povelje kojima se jamči zaštita privatnog i obiteljskog života, zaštita osobnih podataka i pravo na djelotvoran pravni lijek. U tom pogledu Sud navodi da je tom odlukom propisana, kao u Odluci 2000/520, nadređenost zahtjeva u pogledu nacionalne sigurnosti, javnog interesa ili poštovanja američkog zakonodavstva, čime se omogućuje zadiranje u temeljna prava osoba čiji se osobni podaci prenose u tu treću zemlju. Sud smatra da ograničenja zaštite osobnih podataka koja proizlaze iz domaćih propisa SAD-a u vezi s pristupom takvim podacima prenesenima iz Unije u tu treću zemlju i njihovom uporabom od strane američkih tijela, a koja je Komisija ocijenila u Odluci 2016/1250, nisu uređena tako da bi ispunjavala zahtjeve koji su bitno ekvivalentni onima koji se u pravu Unije zahtijevaju na temelju načela proporcionalnosti, s obzirom na to da programi nadzora temeljeni na tim propisima nisu ograničeni na ono što je strogo nužno. Oslanjajući se na utvrđenja u toj odluci, Sud navodi da, kad je riječ o određenim programima nadzora, iz navedenih propisa ne proizlaze nikakva ograničenja u njima sadržanih ovlasti za provođenje tih programa kao ni zaštitne mjere za osobe koje nisu američki državljani, a na koje bi se ti programi mogli odnositi. Sud dodaje da, iako se istim propisima predviđaju zahtjevi koje američka tijela moraju poštovati prilikom provedbe predmetnih programa nadzora, oni osobama na koje se podaci odnose ne dodjeljuju prava na koja se u postupku pred sudovima mogu pozivati protiv američkih tijela.

Kad je riječ o zahtjevu sudske zaštite, Sud presuđuje da, protivno onomu što je Komisija utvrdila u Odluci 2016/1250, mehanizam pravobranitelja predviđen tom odlukom ne jamči tim osobama pravno sredstvo pred tijelom koje nudi zaštitne mjere bitno ekvivalentne onima koje se zahtijevaju pravom Unije, a koje bi mogle osigurati kako neovisnost pravobranitelja predviđenu tim mehanizmom tako i postojanje pravila koja

bi navedenom pravobranitelju omogućila donošenje odluka obvezujućih za američke obavještajne službe. Zbog svih navedenih razloga Sud Odluku 2016/1250 proglašava nevaljanom.

V. Zaštita osobnih podataka na internetu

1. Pravo na prigovor protiv obrade osobnih podataka („pravo na zaborav”)

Presuda od 13. svibnja 2014. (veliko vijeće), Google Spain i Google (C-131/12, EU:C:2014:317)

Sud je u toj presudi (vidjeti također poglavlja II.1. i II.3., naslovljena „Područje primjene općih propisa” i „Pojam ‚obrada osobnih podataka’”) pojasnio doseg prava na pristup i prigovor protiv obrade osobnih podataka na internetu, koja su propisana Direktivom 95/46.

Odgovarajući na pitanje opsega odgovornosti operatora internetskog pretraživača, Sud u biti presuđuje da je – u cilju poštovanja prava na pristup i prigovor, koja su zajamčena člankom 12. točkom (b) i člankom 14. prvim stavkom točkom (a) Direktive 95/46 – kad su stvarno ispunjeni njima predviđeni uvjeti, taj operator u određenim slučajevima obvezan izbrisati s popisa rezultata, prikazanog nastavno na izvršenu pretragu o imenu osobe, poveznice prema mrežnim stranicama koje su objavile treće strane i koje sadržavaju informacije u vezi s tom osobom. Sud pojašnjava da takva obveza može postojati i pod pretpostavkom da to ime ili te informacije nisu prethodno ili istodobno izbrisani s tih mrežnih stranica i to, ovisno o slučaju, čak i kad je njihovo objavljivanje na navedenim stranicama samo po sebi zakonito.

Osim toga, upitan o tome dopušta li se Direktivom ispitaniku da zatraži da se poveznice na internetske stranice uklone s takvog popisa rezultata zato što želi da se navedene informacije koje se odnose na njegovu osobu „zaborave” nakon određenog vremena, Sud najprije ističe da čak i u početku zakonita obrada točnih podataka može s vremenom postati neusklađena s tom direktivom ako ti podaci više nisu nužni s obzirom na svrhe radi kojih su bili prikupljeni ili obrađeni, a osobito kad su ti podaci neprikladni, kad nisu relevantni odnosno nisu više relevantni ili kad su pretjerani u odnosu na te svrhe ili vrijeme koje je proteklo. Stoga, ako se nastavno na zahtjev ispitanika utvrdi da je uključenje tih poveznica u popis rezultata u trenutačnom stanju neusklađeno s Direktivom, informacije i poveznice s tog popisa moraju biti izbrisane. U tom pogledu tvrdnja o postojanju prava ispitanika na to da se informacija koja se odnosi na njegovu osobu više ne povezuje s njegovim imenom na popisu rezultata ne pretpostavlja da uključivanje informacija o kojima je riječ u popis rezultata uzrokuje štetu ispitaniku.

Naposljetku, Sud pojašnjava da – s obzirom na to da ispitanik, imajući u vidu njegova temeljna prava na temelju članaka 7. i 8. Povelje, može zatražiti da se informacija o kojoj je riječ više ne stavlja na raspolaganje širokoj javnosti njezinim uključivanjem u takav

popis rezultata – ta prava načelno prevaguju ne samo nad gospodarskim interesom operatora pretraživača nego i nad interesom javnosti u vezi s pronalaženjem navedene informacije prilikom pretrage o imenu tog ispitanika. Međutim, to ne bi bio slučaj ako je zbog posebnih razloga, kao što je to uloga navedenog ispitanika u javnom životu, zadiranje u njegova temeljna prava opravdano prevagujućim javnim interesom da se takvim uključivanjem ima pristup informaciji o kojoj je riječ.

2. Obrada osobnih podataka i prava intelektualnog vlasništva

Presuda od 29. siječnja 2008. (veliko vijeće), Promusicae (C-275/06, EU:C:2008:54)

Promusicae, španjolsko neprofitno udruženje koje okuplja producente i urednike audiovizualnih i glazbenih zapisa, pokrenulo je pred španjolskim sudovima postupak kako bi se društvu Telefónica de España SAU (trgovačko društvo s djelatnošću, među ostalim, pružanja usluga pristupa internetu) naložilo otkrivanje identiteta i fizičke adrese određenih osoba kojima je to društvo pružalo uslugu pristupa internetu i čiji su adresa IP-a te dan i vrijeme spajanja na internet bili poznati. Prema tvrdnjama udruženja Promusicae, te su se osobe koristile računalnim „peer-to-peer" odnosno „P2P" programom za razmjenu datoteka (transparentno sredstvo za dijeljenje sadržaja koje je neovisno, decentralizirano i posjeduje napredne funkcije pretraživanja i preuzimanja) te su u dijeljenim mapama na svojem osobnom računalu omogućavale pristup fonogramima čija su imovinska prava iskorištavanja pripadala članovima udruženja Promusicae. To je udruženje stoga zatražilo da mu se priopće te informacije kako bi moglo pokrenuti građanske postupke protiv dotičnih osoba.

U tim je okolnostima Juzgado de lo Mercantil nº 5 de Madrid (Trgovački sud br. 5 u Madridu, Španjolska) zatražio od Suda odgovor na pitanje nalaže li se europskim propisima državama članicama propisivanje obveze priopćavanja osobnih podataka u okviru građanskog postupka radi osiguranja djelotvorne zaštite autorskog prava.

Prema stajalištu Suda, navedeni zahtjev za prethodnu odluku odnosi se na problematiku nužnog pomirenja zahtjeva povezanih sa zaštitom različitih temeljnih prava, odnosno, s jedne strane, prava na poštovanje privatnog života i, s druge strane, prava na zaštitu vlasništva i prava na djelotvoran pravni lijek.

Sud u tom pogledu zaključuje da se direktivama 2000/31/EZ o određenim pravnim aspektima usluga informacijskog društva, posebno elektroničkom poslovanju, na unutarnjem tržištu (Direktiva o elektroničkoj trgovini)[83], 2001/29/EZ o usklađivanju

[83] Direktiva 2000/31/EZ Europskog parlamenta i Vijeća od 8. lipnja 2000. o određenim pravnim aspektima usluga informacijskog društva na unutarnjem tržištu, posebno elektroničke trgovine (Direktiva o elektroničkoj trgovini) (SL 2000., L 178, str. 1.) (SL, posebno izdanje na hrvatskom jeziku, poglavlje 13., svezak 39., str. 58.)

određenih aspekata autorskog i srodnih prava u informacijskom društvu[84], 2004/48/EZ o provedbi prava intelektualnog vlasništva[85] i 2002/58 ne nalaže državama članicama propisivanje, u situaciji poput one u glavnom predmetu, obveze priopćavanja osobnih podataka radi osiguranja djelotvorne zaštita autorskog prava u okviru građanskog postupka. Međutim, pravo Unije zahtijeva od navedenih država da te direktive prilikom prenošenja tumače na način koji osigurava pravednu ravnotežu između različitih temeljnih prava zaštićenih pravnim poretkom Zajednice. Nadalje, prilikom provedbe mjera za prenošenje tih direktiva na tijelima i sudovima država članica je ne samo da tumače svoje nacionalno pravo na način koji je u skladu s tim direktivama nego i da se skrbe da ih ne tumače na način koji bi bio u sukobu s navedenim temeljnim pravima ili drugim općim načelima prava Zajednice, kao što je to načelo proporcionalnosti.

Presuda od 19. travnja 2012., Bonnier Audio i dr. (C-461/10, EU:C:2012:219)

Högsta domstolen (Vrhovni sud, Švedska) pokrenuo je prethodni postupak pred Sudom radi tumačenja direktiva 2002/58 i 2004/48 u okviru spora između, s jedne strane, društava Bonnier Audio AB, Earbooks AB, Norstedts Förlagsgrupp AB, Piratförlaget AB i Storyside AB (u daljnjem tekstu: društva Bonnier Audio i dr.) te, s druge strane, društva Perfect Communication Sweden AB (u daljnjem tekstu: društvo ePhone) u vezi sa zahtjevom društava Bonnier Audio i dr. da se društvu ePhone izda nalog za priopćavanje podataka, a čemu se potonje protivi.

U ovom su slučaju izdavačka društva Bonnier Audio i dr. bila nositelji, među ostalim, isključivih prava reproduciranja, izdavanja i stavljanja na raspolaganje javnosti 27 djela u obliku audioknjiga. Ona su smatrala da su njihova isključiva prava povrijeđena javnom difuzijom tih 27 djela, za što ona nisu dala svoju privolu, a koja je provedena posredstvom poslužitelja FTP („*file transfer protocol*”) kojim je omogućeno dijeljenje datoteka i prijenos podataka između računala spojenih na internet. Stoga su ona pokrenula postupak pred švedskim sudovima sa zahtjevom za izdavanje naloga radi priopćavanja imena i adrese osobe koja se koristila adresom IP-a za koju je postojala pretpostavka da su s nje bile prenesene predmetne datoteke.

U tom je kontekstu Högsta domstolen, postupajući u kasacijskom postupku, postavio Sudu upit o tome je li pravu Unije protivna primjena odredbe nacionalnog prava donesene na temelju članka 8. Direktive 2004/48, kojom je u svrhu identifikacije pretplatnika bilo dopušteno u građanskom postupku naložiti pružatelju pristupa internetu da priopći nositelju autorskog prava ili njegovu ovlašteniku identitet pretplatnika kojem je bila dodijeljena adresa IP-a koja je poslužila za povredu navedenog prava. S jedne strane, pretpostavljalo se da su u pogledu podnositelja zahtjeva za izdavanje naloga ispunjene stvarne naznake povrede autorskog prava i, s druge strane, da je zatražena mjera bila proporcionalna.

---

[84] Direktiva 2001/29/EZ Europskog parlamenta i Vijeća od 22. svibnja 2001. o usklađivanju određenih aspekata autorskog i srodnih prava u informacijskom društvu (SL 2001., L 167, str. 10.) (SL, posebno izdanje na hrvatskom jeziku, poglavlje 17., svezak 1., str. 119.)

[85] Direktiva 2004/48/EU Europskog parlamenta i Vijeća od 29. travnja 2004. o provedbi prava intelektualnog vlasništva (SL 2004., L 157, str. 45.) (SL, posebno izdanje na hrvatskom jeziku, poglavlje 17., svezak 2., str. 74.)

Sud prije svega podsjeća na to da članku 8. stavku 3. Direktive 2004/48, u vezi s člankom 15. stavkom 1. Direktive 2002/58, nije protivno to da države članice utvrde obvezu prijenosa privatnim subjektima osobnih podataka kako bi se pred građanskim sudovima omogućilo pokretanje postupaka protiv povreda autorskog prava, ali se njime i ne obvezuje te države da propišu takvu obvezu. Međutim, na tijelima i sudovima država članica jest ne samo da tumače svoje nacionalno pravo na način koji je u skladu s tim direktivama nego i da se skrbe da ga ne tumače na način koji bi bio u sukobu s navedenim temeljnim pravima ili drugim općim načelima prava Unije, kao što je to načelo proporcionalnosti.

U tom pogledu Sud utvrđuje da se predmetnim nacionalnim zakonodavstvom izdavanje naloga za priopćavanje predmetnih podataka uvjetovalo, među ostalim, postojanjem stvarnih naznaka povrede prava intelektualnog vlasništva u pogledu djela, mogućnošću da zatražene informacije olakšaju istragu o povredi ili ugrožavanju autorskog prava i okolnošću da razlozi kojima se obrazlaže takav nalog prevladavaju nepogodnosti ili druge štete koje bi mogle biti prouzročene adresatu tog naloga odnosno interesu koji mu se protivi.

Stoga Sud zaključuje da direktivama 2002/58 i 2004/48 nije protivno nacionalno zakonodavstvo poput onoga o kojem je riječ u glavnom postupku, ako se tim zakonodavstvom nacionalnom sudu koji postupa povodom zahtjeva za izdavanje naloga za priopćavanje osobnih podataka koji je podnijela osoba s pravnim interesom omogućava odvagivanje postojećih suprotstavljenih interesa s obzirom na okolnosti svakog slučaja uz valjano uzimanje u obzir zahtjeva koji proizlaze iz načela proporcionalnosti.

3. Uklanjanje poveznica na osobne podatke

Presuda od 24. rujna 2019. (veliko vijeće), GC i dr. (Uklanjanje poveznica na osjetljive podatke) (C-136/17, EU:C:2019:773)

Sud je u ovoj presudi, odlučujući u velikom vijeću, pojasnio obveze operatora pretraživača u okviru zahtjeva za uklanjanje poveznica koje se odnose na osjetljive podatke.

Google je odbio prihvatiti zahtjeve četiriju osoba da s popisa rezultata koji se prikazuje na pretraživaču nakon izvršene pretrage po njihovim osobnim imenima ukloni različite poveznice prema mrežnim stranicama što su ih objavile treće osobe, osobito prema novinskim člancima. Nakon što su te četiri osobe podnijele pritužbe, Commission nationale de l'informatique et des libertés (Državna komisija za informatičke tehnologije i slobode, CNIL) (Francuska) odbio je naložiti Googleu da provede zatražena uklanjanja poveznica. Conseil d'État (Državno vijeće, Francuska), koji je zatim postupao u predmetu, zatražio je od Suda da pojasni obveze operatora pretraživača prilikom obrade zahtjeva za uklanjanje poveznica na temelju Direktive 95/46.

Kao prvo, Sud podsjeća na to da su obrada osobnih podataka kojima se otkrivaju rasno ili etničko podrijetlo, politička mišljenja, vjerska ili filozofska uvjerenja i članstvo u sindikatu kao i obrada podataka u vezi sa zdravljem ili spolnim životom zabranjene[86], uz određene iznimke i odstupanja. Kada je riječ o obradi podataka koji se odnose na kaznena djela, kaznene osude i sigurnosne mjere, ona se može izvršiti jedino pod nadzorom službenog tijela ili ako su nacionalnim pravom predviđene prikladne i posebne mjere[87].

Sud ocjenjuje da se zabrana i ograničenja koji se odnose na obradu tih posebnih kategorija podataka primjenjuju na operatora pretraživača kao i na svakog drugog voditelja obrade osobnih podataka. Naime, cilj je tih zabrana i ograničenja osiguravanje pojačane zaštite od takvih obrada, koje, zbog posebne osjetljivosti tih podataka, mogu predstavljati osobito teško zadiranje u temeljna prava na poštovanje privatnog života i zaštite osobnih podataka.

Međutim, operator pretraživača nije odgovoran za to što se osobni podaci nalaze na mrežnoj stranici koju je objavila treća osoba, nego za postavljanje poveznice prema toj stranici. U tim okolnostima, zabrana i ograničenja koji se odnose na obradu osjetljivih podataka primjenjuju se na tog operatora samo zbog tog postavljanja te stoga provjerom koju valja provesti na temelju ispitanikova zahtjeva i pod nadzorom nadležnih nacionalnih tijela.

Kao drugo, Sud ocjenjuje da, kada operator odlučuje o zahtjevu za uklanjanje poveznica prema osjetljivim podacima načelno ga je dužan prihvatiti, uz određene iznimke. Kada je riječ o tim iznimkama, operator može, među ostalim, odbiti takav zahtjev ako utvrdi da poveznice vode prema podacima za koje je očito da ih je objavio ispitanik[88], pod uvjetom da postavljanje takvih poveznica zadovoljava ostale uvjete zakonitosti obrade osobnih podataka, osim ako ispitanik ima pravo prigovora na postavljanje tih poveznica zbog razloga koji se tiču njegove posebne situacije[89].

U svakom slučaju, kada odlučuje o zahtjevu za uklanjanje poveznica, operator pretraživača mora provjeriti je li uključivanje poveznice prema mrežnoj stranici na kojoj su objavljeni osjetljivi podaci u popis rezultata prikazan nakon pretrage po osobnom imenu te osobe strogo nužno za zaštitu slobode informiranja internetskih korisnika potencijalno zainteresiranih da posredstvom navedene pretrage pristupe toj mrežnoj stranici. U tom pogledu Sud naglašava da, iako prava na privatnost i na zaštitu osobnih podataka općenito prevaguju nad slobodom informiranja internetskih korisnika, ta ravnoteža u posebnim slučajevima ipak može ovisiti o naravi informacije o kojoj je riječ, o njezinoj osjetljivosti u odnosu na ispitanikov privatni život kao i o javnom interesu za tu informaciju, koji se može razlikovati osobito s obzirom na ulogu koju ta osoba ima u javnom životu.

---

86 Članak 8. stavak 1. Direktive 95/46 i članak 9. stavak 1. Uredbe 2016/679

87 Članak 8. stavak 5. Direktive 95/46 i članak 10. Uredbe 2016/679

88 Članak 8. stavak 2. točka (e) Direktive 95/46 i članak 9. stavak 2. točka (e) Uredbe 2016/679

89 Članak 14. prvi stavak točka (a) Direktive 95/46 i članak 21. stavak 1. Uredbe 2016/679

Kao treće, Sud zaključuje da je – u okviru zahtjeva za uklanjanje poveznica prema mrežnim stranicama na kojima su objavljene informacije o pravosudnom postupku u kaznenim stvarima vođenom protiv ispitanika koje se tiču ranije faze tog postupka i više ne odgovaraju trenutačnoj situaciji – na operatoru pretraživača da procijeni ima li navedena osoba, s obzirom na sve okolnosti predmetnog slučaja, pravo na to da se informacije o kojima je riječ u trenutačnom stanju više ne povezuju s njezinim osobnim imenom na popisu rezultata prikazanom nakon pretrage po tom imenu. Međutim, čak i ako to nije slučaj zato što se uključivanje poveznice o kojoj je riječ pokazuje strogo nužnim za usklađivanje ispitanikova prava na privatnost i na zaštitu osobnih podataka sa slobodom informiranja potencijalno zainteresiranih internetskih korisnika, operator je dužan, najkasnije povodom zahtjeva za uklanjanje poveznica, urediti popis rezultata na takav način da opća slika koju taj popis pruža internetskom korisniku odražava trenutačnu pravosudnu situaciju, što osobito zahtijeva da se poveznice prema mrežnim stranicama koje sadržavaju informacije o toj temi nađu na vrhu spomenutog popisa.

Presuda od 24. rujna 2019. (veliko vijeće), Google (Teritorijalni doseg uklanjanja poveznica) (C-507/17,* EU:C:2019:772*)

Commission nationale de l'informatique et des libertés (Državna komisija za informatičke tehnologije i slobode, CNIL) (Francuska) naložila je Googleu da, kad prihvati zahtjev za uklanjanje poveznica koje se prikažu nakon pretrage po ispitanikovu osobnom imenu, s popisa rezultata ukloni poveznice koje upućuju na internetske stranice koje sadržavaju njegove osobne podatke na svim nastavcima naziva domene tog pretraživača. Nakon što Google nije postupio u skladu s tim nalogom, CNIL mu je izrekao sankciju od 100 000 eura. Conseil d'État (Državno vijeće, Francuska), kojemu se Google obratio, zatražio je od Suda pojašnjenje teritorijalnog dosega obveze operatora pretraživača da provede pravo na uklanjanje poveznica u skladu s Direktivom 95/46.

Sud najprije podsjeća na mogućnost fizičkih osoba da na temelju prava Unije ostvare svoje pravo na uklanjanje poveznica prema operatoru pretraživača koji ima jedan poslovni nastan ili više njih na području Unije, neovisno o činjenici odvija li se obrada osobnih podataka (u ovom slučaju poveznice prema internetskim stranicama na kojima se nalaze osobni podaci osobe koja se poziva na to pravo) u Uniji ili ne[90].

Kad je riječ o dosegu prava na uklanjanje poveznica, Sud smatra da operator pretraživača nije dužan provesti uklanjanje poveznica na svim verzijama svojeg pretraživača, nego na njegovim verzijama koje odgovarajuće postoje u svim državama članicama. U tom pogledu ističe da, iako bi sveopće uklanjanje poveznica s obzirom na karakteristike interneta i pretraživača u potpunosti ispunilo cilj zakonodavca Unije da se osigura visoka razina zaštite osobnih podataka u cijeloj Uniji, iz prava Unije[91] ipak ni na koji način ne proizlazi da je zakonodavac radi ostvarenja tog cilja pravu na uklanjanje poveznica odabrao dati doseg koji bi prelazio državno područje država članica.

[90] Članak 4. stavak 1. točka (a) Direktive 95/46 i članak 3. stavak 1. Uredbe 2016/679

[91] Članak 12. točka (b) i članak 14. prvi stavak točka (a) Direktive 95/46 i članak 17. stavak 1. Uredbe 2016/679

Konkretno, iako pravo Unije uspostavlja mehanizme suradnje između nadzornih tijela država članica kako bi se postigla zajednička odluka, koja se temelji na odvagivanju između prava na zaštitu privatnosti i osobnih podataka, s jedne strane, i interesa javnosti u različitim državama članicama na pristup informacijama, s druge strane, u pogledu dosega uklanjanja poveznica izvan Unije takvi mehanizmi trenutačno nisu predviđeni.

Prema trenutačnom stanju prava Unije, na operatoru pretraživača jest da provede traženo uklanjanje poveznica, i to ne samo na verziji pretraživača koja odgovarajuće postoji u državi članici rezidentnosti korisnika tog uklanjanja, nego na verzijama pretraživača koje odgovarajuće postoje u državama članicama, i to kako bi se osigurala dosljedna i visoka razina zaštite u cijeloj Uniji. Osim toga, na takvom je operatoru da, ako je to potrebno, poduzme dovoljno učinkovite mjere kako bi spriječio ili barem ozbiljno obeshrabrio internetske korisnike u Uniji da, ovisno o slučaju, s verzije pretraživača koja odgovarajuće postoji u trećoj zemlji pristupe poveznicama koje su predmet uklanjanja poveznica te je na nacionalnom sudu da provjeri ispunjavaju li mjere koje je operator usvojio taj zahtjev.

Naposljetku, Sud naglašava da, iako pravo Unije ne nameće operatoru obvezu provedbe uklanjanja poveznica na svim verzijama njegova pretraživača, ono ga ni ne zabranjuje. Prema tome, nadzorno tijelo ili sudsko tijelo države članice ostaje nadležno za provedbu, s obzirom na nacionalne standarde zaštite temeljnih prava, odvagivanja između prava ispitanika na poštovanje njegove privatnosti i na zaštitu njegovih osobnih podataka, s jedne strane, i prava na slobodu informiranja, s druge strane, te, nakon tog odvagivanja, za nalaganje, prema potrebi, operatoru tog pretraživača da ukloni poveznice na svim njegovim verzijama.

Presuda od 8. prosinca 2022. (veliko vijeće), Google (Uklanjanje poveznica koje vode do navodno netočnog sadržaja) (C-460/20, EU:C:2022:962)

Tužitelji u glavnom postupku, osoba TU, koji radi na odgovornim pozicijama i drži udjele u različitim društvima, i osoba RE, koja je bila njegova izvanbračna partnerica te do svibnja 2015. prokuristica jednog od tih društava, bili su tema triju članaka koja je 2015. na jednoj internetskoj stranici objavilo društvo G LLC, koje upravlja tom stranicom. Ti su članci, od kojih je jedan bio ilustriran četirima fotografijama koje su prikazivale tužitelje i sugerirale da vode luksuzan život, kritizirali model ulaganja nekoliko njihovih društava. Pristup tim člancima bio je moguć pretraživanjem u pretraživaču kojim upravlja društvo Google LLC (u daljnjem tekstu: Google) imena i prezimena tužiteljâ, kako izdvojeno tako i zajedno s određenim nazivima društava. Popis rezultata upućivao je na te članke putem poveznice kao i na fotografije prikazane u obliku minijatura („*thumbnails*”).

Tužitelji u glavnom postupku zatražili su od Googlea, kao voditelja obrade osobnih podataka koja se provodi putem njegova pretraživača, s jedne strane, da s popisa rezultata pretraživanja ukloni poveznice na sporne članke zbog toga što sadržavaju netočne tvrdnje i klevetnička mišljenja te, s druge strane, da s popisa rezultata pretraživanja ukloni minijature. Google je odbio prihvatiti taj zahtjev.

Nakon što je njihov zahtjev odbijen kako u prvostupanjskom tako i u žalbenom postupku, tužitelji u glavnom postupku podnijeli su reviziju Bundesgerichtshofu (Savezni vrhovni sud, Njemačka), u okviru koje je Bundesgerichtshof Sudu uputio zahtjev za prethodnu odluku u pogledu tumačenja OUZP-a i Direktive 95/46[92].

Svojom presudom, donesenom u velikom vijeću, Sud razvija svoju sudsku praksu o uvjetima koji se primjenjuju na zahtjeve za uklanjanje poveznica podnesene operatoru pretraživača na temelju pravila o zaštiti osobnih podataka. Konkretno, on ispituje, s jedne strane, opseg obveza i odgovornosti koje operator pretraživača ima prilikom obrade zahtjeva za uklanjanje poveznica koji se temelji na navodnoj netočnosti informacija sadržanih u indeksiranom sadržaju i, s druge strane, teret dokazivanja ispitanika u pogledu te netočnosti. Osim toga, on se izjašnjava o potrebi uzimanja u obzir prvotnog konteksta objave fotografija na internetu u svrhu ispitivanja zahtjeva za uklanjanje fotografija prikazanih u obliku minijatura na popisu rezultata pretraživanja slika.

Kao prvo, Sud je presudio da, u okviru odvagivanja između, s jedne strane, pravâ na poštovanje privatnog života i zaštitu osobnih podataka i, s druge strane, prava na slobodu izražavanja i informiranja[93], u svrhu ispitivanja zahtjeva za uklanjanje poveznica koji je podnesen operatoru pretraživača i kojim se traži uklanjanje s popisa rezultata pretraživanja poveznice koja vodi na sadržaj koji sadržava navodno netočne informacije, to uklanjanje poveznica nije podvrgnuto uvjetu da je pitanje točnosti indeksiranog sadržaja bilo riješeno barem privremeno u okviru tužbe koju je podnio podnositelj zahtjeva protiv pružatelja sadržaja.

Uvodno, u svrhu ispitivanja pod kojim je uvjetima operator pretraživača dužan prihvatiti zahtjev za uklanjanje poveznica i stoga obrisati s popisa rezultata koji se prikazuje nakon pretrage ispitanikova osobnog imena poveznicu prema internetskoj stranici na kojoj se nalaze tvrdnje koje ta osoba smatra netočnima, Sud je, među ostalim, podsjetio na sljedeće:

• u mjeri u kojoj aktivnost pretraživača može, u odnosu na aktivnost urednikâ internetskih stranica, znatno i dodatno utjecati na temeljna prava na privatnost i na zaštitu osobnih podataka, operator tog pretraživača, kao osoba koja određuje svrhe i načine te aktivnosti, mora u okviru svojih odgovornosti, nadležnosti i mogućnosti osigurati da jamstva iz Direktive 95/46 i OUZP-a mogu razviti svoj puni učinak i da se može ostvariti učinkovita i potpuna zaštita ispitanika;

• operator pretraživača, koji odlučuje o zahtjevu za uklanjanje poveznica, mora provjeriti je li uključivanje poveznice na internetsku stranicu o kojoj je riječ u popis rezultata nužno za ostvarivanje prava na slobodu informiranja internetskih korisnika potencijalno zainteresiranih da posredstvom navedene pretrage pristupe toj internetskoj stranici, zaštićenog pravom na slobodu izražavanja i informiranja;

---

92 Članak 17. stavak 3. točka (a) OUZP-a odnosno članak 12. točka (b) i članak 14. prvi stavak točka (a) Direktive 95/46

93 Temeljna prava zajamčena člancima 7., 8. i 11. Povelje

• OUZP izričito postavlja zahtjev odvagivanja između, s jedne strane, temeljnih prava na privatnost i na zaštitu osobnih podataka i, s druge strane, temeljnog prava na slobodu informiranja.

Sud najprije ističe da, iako ispitanikova prava na zaštitu privatnog života i zaštitu osobnih podataka općenito prevaguju nad legitimnim interesom internetskih korisnika za pristup informacijama o kojima je riječ, ta ravnoteža ipak može ovisiti o relevantnim okolnostima svakog slučaja, osobito o naravi te informacije i njezinoj osjetljivosti za privatni život ispitanika kao i o interesu javnosti za tu informaciju, koji se može razlikovati osobito s obzirom na ulogu koju ta osoba ima u javnom životu.

Pitanje je li indeksirani sadržaj točan ili ne čini također relevantan element u okviru te ocjene. Tako u određenim okolnostima pravo na informiranje internetskih korisnika i sloboda izražavanja pružatelja sadržaja mogu prevagnuti nad pravima na zaštitu privatnog života i zaštitu osobnih podataka, osobito kada ispitanik ima ulogu u javnom životu. Međutim, taj se odnos obrće kada se barem dio informacija na koje se odnosi zahtjev za uklanjanje poveznica, a koji nije neznatan s obzirom na cijeli sadržaj, pokaže netočnim. U takvom slučaju pravo na informiranje i pravo na dobivanje informacija ne mogu se uzeti u obzir jer ne mogu uključivati pravo širenja takvih informacija i pristupa njima.

Nadalje, što se tiče, s jedne strane, obveza u vezi s dokazivanjem netočnosti informacija u indeksiranom sadržaju, Sud pojašnjava da je osoba koja zahtijeva uklanjanje poveznica, zbog netočnosti tih informacija, dužna dokazati očitu netočnost tih informacija ili barem jednog dijela tih informacija koji nije neznatan s obzirom na taj cijeli sadržaj. Međutim, kako bi se izbjeglo to da se toj osobi stavi prekomjeran teret koji može naštetiti korisnom učinku prava na uklanjanje poveznica, na njoj je samo da podnese dokaze za koje se, s obzirom na okolnosti predmetnog slučaja, od nje može razumno zahtijevati da ih istraži. Ta osoba u načelu ne može biti dužna već u predsudskoj fazi, u prilog svojem zahtjevu za uklanjanje poveznica, podnijeti sudsku odluku donesenu protiv urednika internetske stranice, čak i u obliku odluke o privremenoj pravnoj zaštiti.

S druge strane, što se tiče obveza i odgovornosti operatora pretraživača, Sud ističe da se on, kako bi provjerio može li sadržaj i dalje biti uključen u popis rezultata pretraživanja koje se provodi putem njegova pretraživača nakon zahtjeva za uklanjanje poveznica, mora temeljiti na svim predmetnim pravima i interesima kao i na svim okolnostima slučaja. Međutim, taj operator ne može biti dužan istražiti činjenice i u tu svrhu organizirati kontradiktornu razmjenu s pružateljem sadržaja u svrhu pribavljanja elemenata koji nedostaju u vezi s točnošću indeksiranog sadržaja. Obveza pridonošenja dokazivanju je li indeksirani sadržaj točan ili ne tom bi operatoru nametala teret koji prelazi ono što se od njega može razumno očekivati u pogledu njegovih odgovornosti, nadležnosti i mogućnosti. To bi rješenje podrazumijevalo ozbiljnu opasnost od uklanjanja poveznica na sadržaj koji zadovoljava potrebu za legitimnim informacijama za koje postoji prevladavajući javni interes i da tako postane teško pronaći ga na internetu. Stoga bi postojala stvarna opasnost od odvraćajućeg učinka na ostvarivanje slobode izražavanja i informiranja ako bi takav operator uklanjanje poveznica obavljao na gotovo

sustavan način kako bi izbjegao snošenje troškova istraživanja činjenica koje su relevantne za utvrđivanje točnosti indeksiranog sadržaja.

Stoga je operator pretraživača dužan prihvatiti taj zahtjev za uklanjanje poveznica ako osoba koja je podnijela zahtjev za uklanjanje poveznica podnese dokaze koji mogu potkrijepiti njezin zahtjev i dokazati netočnost informacija iz indeksiranog sadržaja ili barem jednog dijela tih informacija koji nije neznatan s obzirom na cijeli taj sadržaj. Isto vrijedi i kada taj podnositelj zahtjeva podnese sudsku odluku protiv urednika internetske stranice koja se temelji na utvrđenju da su informacije sadržane u indeksiranom sadržaju, koje nisu neznatne s obzirom na cijeli sadržaj, barem na prvi pogled netočne. Nasuprot tomu, ako iz dokaza koje je pružio podnositelj zahtjeva nije očito vidljivo da su te informacije netočne, operator pretraživača nije dužan u slučaju nepostojanja takve sudske odluke prihvatiti taj zahtjev za uklanjanje poveznica. Kada informacije o kojima je riječ mogu pridonijeti raspravi u općem interesu, s obzirom na sve okolnosti predmetnog slučaja, valja pridati osobitu važnost pravu na slobodu izražavanja i informiranja.

Naposljetku, Sud dodaje da, ako operator pretraživača ne postupi po zahtjevu za uklanjanje poveznica, ispitanik mora imati mogućnost obratiti se nadzornom tijelu ili sudskom tijelu radi provedbe nužnih provjera i nalaganja tom voditelju obrade odgovarajućih mjera. U tom smislu osobito je na sudskim tijelima da osiguraju odvagivanje suprotstavljenih interesa, s obzirom na to da su ona u najboljem položaju za provedbu složenog i dubinskog odvagivanja, koje uzima u obzir sve kriterije i elemente utvrđene relevantnom sudskom praksom.

Kao drugo, Sud presuđuje da, u okviru odvagivanja navedenih prava, radi ispitivanja zahtjeva za uklanjanje poveznica kojim se traži da se iz rezultata pretraživanja slika koje je izvršeno na temelju imena fizičke osobe uklone fotografije prikazane u obliku minijatura na kojima se nalazi ta osoba, treba uzeti u obzir informativnu vrijednost tih fotografija neovisno o kontekstu njihove objave na internetskoj stranici iz koje su izdvojene. Međutim, treba uzeti u obzir sve tekstualne elemente koji izravno prate prikazivanje tih fotografija u rezultatima pretraživanja i koji mogu pojasniti njihovu informativnu vrijednost.

Kako bi došao do tog zaključka, Sud ističe da se na pretraživanja slika putem internetskog pretraživača na temelju imena osobe primjenjuju ista načela kao što su ona koja se primjenjuju na pretraživanja internetskih stranica i informacija koje su na njima sadržane. Ističe da prikazivanje, nakon pretraživanja na temelju imena, u obliku minijatura, fotografija ispitanika čini osobito veliko miješanje u prava na zaštitu privatnosti i osobnih podataka te osobe.

Prema tome, kada je operatoru pretraživača podnesen zahtjev za uklanjanje poveznica s ciljem uklanjanja iz rezultata pretraživanja slika izvršenog na temelju imena osobe fotografija prikazanih u obliku minijatura koje prikazuju tu osobu, on mora provjeriti je li prikazivanje predmetnih fotografija nužno za ostvarivanje prava na slobodu informiranja internetskih korisnika koji su potencijalno zainteresirani za pristup tim fotografijama putem takvog pretraživanja.

Međutim, budući da pretraživač prikazuje fotografije ispitanika izvan konteksta u kojem su objavljene na internetskoj stranici na koju se upućuje, najčešće kako bi se ilustrirali tekstualni elementi koje ta stranica sadržava, valja utvrditi treba li taj kontekst ipak uzeti u obzir prilikom odvagivanja suprotstavljenih prava i interesa koje treba provesti. U tom okviru pitanje mora li navedena ocjena uključivati i sadržaj internetske stranice na kojoj se nalazi fotografija za koju se traži uklanjanje prikaza u obliku minijature ovisi o predmetu i naravi obrade o kojoj je riječ.

Što se tiče, kao prvo, predmeta obrade o kojoj je riječ, Sud ističe da objava fotografija kao neverbalnog sredstva komunikacije može imati snažniji utjecaj na internetske korisnike nego tekstualne objave. Naime, fotografije su kao takve važno sredstvo za privlačenje pažnje internetskih korisnika i mogu stvoriti interes za pristup člancima koje ilustriraju. Međutim, osobito zbog okolnosti da se one često mogu tumačiti na više načina, njihovo prikazivanje na popisu rezultata pretraživanja kao minijatura može dovesti do osobito ozbiljnog miješanja u pravo ispitanika na zaštitu njegova ugleda, što treba uzeti u obzir u okviru odvagivanja između suprotstavljenih prava i interesa. Različito odvagivanje nameće se ovisno o tome je li riječ, s jedne strane, o člancima s fotografijama koje je objavio urednik internetske stranice i koje, umetnute u svoj izvorni kontekst, ilustriraju informacije u tim člancima i mišljenja koja su u njima iznesena i, s druge strane, o fotografijama koje u obliku minijatura na popisu rezultata prikazuje operator pretraživača izvan konteksta u kojem su one objavljene na izvornoj internetskoj stranici.

U tom pogledu Sud podsjeća na to da ne samo da se razlog koji opravdava objavu osobnog podatka na internetskoj stranici ne podudara nužno s razlogom koji se primjenjuje na aktivnost pretraživačâ nego, čak i kad je to slučaj, može postojati razlika u odvagivanju dotičnih prava i interesa koje treba provesti, ovisno o tome radi li se o obradi koju izvršava operator pretraživača ili urednik te internetske stranice. S jedne strane, legitimni interesi koji opravdavaju te obrade mogu biti različiti i, s druge strane, posljedice navedenih obrada na ispitanika i posebno njegovu privatnost nisu nužno iste.

Što se tiče, kao drugo, naravi obrade koju provodi operator pretraživača, Sud utvrđuje da preuzimanjem fotografija fizičkih osoba objavljenih na internetu i njihovim odvojenim prikazivanjem, u rezultatima pretraživanja slika u obliku minijatura, operator pretraživača nudi uslugu u okviru koje provodi obradu osobnih podataka koja je samostalna i zasebna u odnosu na obradu koju provodi urednik internetske stranice s koje su preuzete fotografije te na postavljanje poveznica koje vode do te stranice za koje je takav operator također odgovoran.

Slijedom toga, potrebna je samostalna ocjena aktivnosti operatora pretraživača koja se sastoji od prikazivanja rezultata pretraživanja slika u obliku minijatura, s obzirom na to da dodatno zadiranje u temeljna prava koje proizlazi iz takve aktivnosti može biti osobito intenzivno zbog skupljanja, prilikom pretraživanja na temelju imena, svih informacija koje se odnose na ispitanika dostupnih na internetu. U okviru te samostalne ocjene valja uzeti u obzir činjenicu da je to prikazivanje samo po sebi rezultat koji traži internetski korisnik, neovisno o njegovoj naknadnoj odluci o tome hoće li pristupiti izvornoj internetskoj stranici.

Međutim, Sud primjećuje da takvo posebno odvagivanje, koje uzima u obzir samostalnu narav obrade koju provodi operator pretraživača, ne dovodi u pitanje moguću relevantnost tekstualnih elemenata koji mogu izravno pratiti prikaz fotografije na popisu rezultata pretraživanja, s obzirom na to da takvi elementi mogu pojasniti informativnu vrijednost te fotografije za javnost i stoga utjecati na odvagivanje relevantnih prava i interesa.

4. Privola korisnika internetske stranice na pohranu informacija

Presuda od 1. listopada 2019. (veliko vijeće), Planet49 (C-673/17, EU:C:2019:801)

Sud je u ovoj presudi smatrao da privola na pohranu informacija ili pristup informacijama posredstvom kolačića smještenih na terminalnoj opremi korisnika internetske stranice nije dana valjano ako odobrenje proizlazi iz polja koje je unaprijed označeno kvačicom, i to neovisno o činjenici jesu li predmetne informacije osobni podaci. Usto, Sud je naveo da pružatelj usluga mora korisniku internetske stranice navesti trajanje kolačića i informaciju imaju li treće osobe mogućnost pristupa tim kolačićima.

Spor u glavnom postupku odnosio se na nagradnu igru koju je društvo Planet49 organiziralo na internetskoj stranici www.dein-macbook.de. Da bi mogli sudjelovati, internetski korisnici morali su unijeti svoje ime i adresu na internetskoj stranici na kojoj su stajala polja za označavanje kvačicom. Polje kojim se dopušta instaliranje kolačića bilo je unaprijed označeno kvačicom. Bundesgerichtshof (Savezni vrhovni sud, Njemačka), pred kojim je njemački Savez udruga potrošača podnio reviziju, izrazio je dvojbu o valjanosti dobivanja privole korisnikâ korištenjem polja koje je unaprijed označeno kvačicom te o opsegu obveze informiranja koja leži na pružatelju usluge.

Zahtjev za prethodnu odluku u bitnome se odnosio na tumačenje pojma „privola” iz Direktive 2002/58[94], u vezi s Direktivom 95/46[95] i OUZP-om[96].

Kao prvo, Sud napominje da se u članku 2. točki (h) Direktive 95/46, na koji upućuje članak 2. točka (f) Direktive 2002/58, privola definira kao „svaka dobrovoljno dana, posebna i informirana izjava volje kojom osoba čiji se podaci obrađuju daje svoju suglasnost da se obrade osobni podaci koji se na nju odnose”. Sud ističe da zahtjev postojanja „izjave” volje osobe čiji se podaci obrađuju jasno upućuje na aktivno, a ne na pasivno djelovanje. No, privola dana poljem koje je unaprijed označeno kvačicom ne uključuje aktivno djelovanje korisnika internetske stranice. Usto, povijest nastanka članka 5. stavka 3. Direktive 2002/58, koji od izmjene provedene Direktivom 2009/136 predviđa da je korisnik morao „da[ti] svoj pristanak” za postavljanje kolačića, upućuje na

[94] Članak 2. točka (f) i članak 5. stavak 3. Direktive 2002/58, kako je izmijenjena Direktivom 2009/136/EZ Europskog parlamenta i Vijeća od 25. studenoga 2009. (SL 2009., L 337, str. 11.) (SL, posebno izdanje na hrvatskom jeziku, poglavlje 13., svezak 52., str. 224. i ispravci SL 2017., L 162, str. 56. i SL 2018., L 74, str. 11.)

[95] Članak 2. točka (h) Direktive 95/46

[96] Članak 6. stavak 1. točka (a) Uredbe 2016/679

to da se korisnikova privola sada više ne može predmnijevati i da mora proizlaziti iz njegova aktivnog djelovanja. Konačno, aktivna privola sada se predviđa OUZP-om[97], čiji članak 4. točka 11. zahtijeva očitovanje volje koje ima oblik, među ostalim, „jasn[e] potvrdn[e] radnj[e]”, a njezina uvodna izjava 32. izričito isključuje postojanje privole u slučaju „[š]utnj[e], unaprijed kvačicom označen[ih] polj[a] ili manj[ka] aktivnosti”.

Sud stoga zaključuje da privola nije dana valjano ako se pohranjivanje informacija ili pristup informacijama već pohranjenima na terminalnoj opremi korisnika internetske stranice putem kolačića dopušta poljem koje je unaprijed označeno kvačicom, a koju korisnik mora ukloniti da bi odbio dati svoju privolu. On dodaje da činjenica da je taj korisnik aktivirao gumb za sudjelovanje u dotičnoj nagradnoj igri ne može biti dovoljna za zaključak da je valjano dao privolu za postavljanje kolačića.

Kao drugo, Sud utvrđuje da članak 5. stavak 3. Direktive 2002/58 ima za cilj zaštititi korisnika od bilo kakvog zadiranja u privatnost, neovisno o tome odnosi li se to zadiranje na osobne podatke. Iz toga slijedi da pojam „privola” ne treba tumačiti različito ovisno o tome jesu li informacije koje se pohranjuju ili pregledavaju na terminalnoj opremi korisnika internetske stranice osobni podaci.

Kao treće, Sud ističe da članak 5. stavak 3. Direktive 2002/58 zahtijeva da je korisnik dao svoju privolu nakon što je iscrpno i razumljivo obaviješten, uz ostalo, o namjeni postupka obrade. Međutim, iscrpne i razumljive informacije trebaju korisniku omogućiti da lako uvidi posljedice mogućeg davanja privole te osigurati da ta privola bude dana imajući na raspolaganju sve činjenice. U tom smislu, Sud smatra da su trajanje kolačića i pitanje imaju li treće osobe mogućnost pristupa tim kolačićima dio iscrpne i razumljive informacije koju pružatelj usluga mora dati korisniku internetske stranice.

5. Obrada osobnih podataka na internetskim društvenim mrežama

Presuda od 4. srpnja 2023. (veliko vijeće), Meta Platforms i dr. (Opći uvjeti uporabe društvene mreže) (C-252/21, EU:C:2023:537)

Društvo Meta Platforms vlasnik je internetske društvene mreže „Facebook”, koja je besplatna za privatne korisnike. Poslovni model te društvene mreže temelji se na financiranju internetskim oglašavanjem koje se prilagođava njegovim pojedinačnim korisnicima. Tako oglašavanje tehnički omogućuje automatizirana izrada vrlo detaljnih profila korisnika mreže i internetskih usluga koje nudi koncern Meta. Stoga, kako bi se mogli koristiti navedenom društvenom mrežom, korisnici u trenutku registracije moraju prihvatiti opće uvjete društva Meta Platforms koji upućuju na pravila o upotrebi podataka i kolačića koje je utvrdilo navedeno društvo. U skladu s potonjima, osim podataka koje ti korisnici izravno pružaju prilikom svoje registracije, Meta Platforms

97 *Idem.*

prikuplja i podatke o aktivnostima navedenih korisnika, u okviru društvene mreže i izvan nje, te ih zatim povezuje s Facebook računima korisnika o kojima je riječ. Što se tiče tih potonjih podataka, također nazvanih „*off* Facebook podaci", riječ je o, s jedne strane, podacima koji se odnose na posjećivanje trećih internetskih stranica i aplikacija i, s druge strane, podacima koji se odnose na uporabu drugih internetskih usluga u vlasništvu koncerna Meta (među kojima su Instagram i WhatsApp). Sveobuhvatan uvid u te podatke omogućuje stvaranje detaljnih zaključaka o sklonostima i interesima tih korisnika.

Odlukom od 6. veljače 2019. Bundeskartellamt (Savezni ured za zaštitu tržišnog natjecanja, Njemačka) zabranio je društvu Meta Platforms, s jedne strane, da uvjetuje, u okviru općih uvjeta koji su tada bili na snazi, privatnim korisnicima koji borave u Njemačkoj uporabu društvene mreže Facebook obradom njihovih *off* Facebook podataka i, s druge strane, da, bez njihove privole, obrađuje te podatke. Usto, Savezni ured za tržišno natjecanje tom je društvu naložio da prilagodi te opće uvjete tako da iz njih jasno proizlazi da navedeni podaci neće biti prikupljeni, povezani s Facebook računima korisnikâ ni upotrijebljeni bez privole korisnika o kojima je riječ. Naposljetku, taj je ured istaknuo da takva privola nije valjana ako je ona uvjet za uporabu društvene mreže. Taj je ured obrazložio svoju odluku činjenicom da obrada podataka korisnika o kojima je riječ, koja nije u skladu s OUZP-om, predstavlja zlouporabu vladajućeg položaja društva Meta Platforms na tržištu internetskih društvenih mreža.

Meta Platforms je podnio tužbu protiv te odluke Oberlandesgerichtu Düsseldorf (Visoki zemaljski sud u Düsseldorfu, Njemačka). Budući da je dvojio, među ostalim, u pogledu tumačenja i primjene određenih odredbi OUZP-a, Oberlandesgericht Düsseldorf uputio je Sudu zahtjev za prethodnu odluku.

Sud, zasjedajući u velikom vijeću, svojom presudom pojašnjava mogućnost operatora društvene mreže da obrađuje „osjetljive" osobne podatke svojih korisnika, uvjete za zakonitost načina na koji takav operator obrađuje podatke i valjanost privole koju ti korisnici daju za takvu obradu podataka poduzeću koje ima vladajući položaj na nacionalnom tržištu internetskih društvenih mreža.

Kad je riječ o obradi posebnih kategorija osobnih podataka[98], Sud smatra da, u slučaju kada korisnik internetske društvene mreže posjećuje internetske stranice ili koristi aplikacije koje su povezane s jednom ili više tih kategorija i, ovisno o slučaju, ondje unosi podatke prilikom registracije ili obavljanjem internetskih narudžbi, način na koji taj operator te internetske društvene mreže obrađuje osobne podatke[99] treba smatrati „obradom posebnih kategorija osobnih podataka", u smislu članka 9. stavka 1. OUZP-a, ako ta obrada podataka omogućuje otkrivanje informacija obuhvaćenih jednom od tih

[98] Na koje se odnosi članak 9. stavak 1. OUZP-a. Ta odredba predviđa da „[se z]abranjuje [...] obrada osobnih podataka koji otkrivaju rasno ili etničko podrijetlo, politička mišljenja, vjerska ili filozofska uvjerenja ili članstvo u sindikatu te obrada genetskih podataka, biometrijskih podataka u svrhu jedinstvene identifikacije pojedinca, podataka koji se odnose na zdravlje ili podataka o spolnom životu ili seksualnoj orijentaciji pojedinca."

[99] Ta se obrada sastoji u prikupljanju, preko sadržanih sučelja, kolačića odnosno slične tehnologije za pohranu, podataka proizišlih iz posjećivanja tih stranica i korištenja tih aplikacija te podataka koje je unio korisnik, u povezivanju svih tih podataka s njegovim računom na društvenoj mreži i u uporabi tog operatora navedenih podataka.

posebnih kategorija, bilo da se te informacije odnose na korisnika te mreže ili na drugu fizičku osobu. Takva je obrada u načelu zabranjena, ne dovodeći u pitanje određena odstupanja[100].

S tim u vezi, Sud pojašnjava da, kada korisnik internetske društvene mreže posjećuje internetske stranice ili koristi aplikacije koje su povezane s jednom ili više navedenih posebnih kategorija podataka, on očito ne objavljuje[101] podatke o tom posjećivanju ili korištenju koje je operator te internetske društvene mreže prikupio preko kolačića ili sličnih tehnologija za pohranu. Osim toga, kada on unese podatke na te stranice ili u te aplikacije ili kada odabere opcije sadržane na tim stranicama ili tim aplikacijama, poput opcija „Sviđa mi se" ili „Podijeli" ili opcija koje korisniku omogućuju da se prijavi na te stranice i u te aplikacije korištenjem podataka za prijavu povezanih s njegovim korisničkim računom na društvenoj mreži, njegovim telefonskim brojem ili njegovom adresom elektroničke pošte, takav korisnik očito objavljuje podatke koji su tako uneseni ili tako proizlaze iz odabira tih opcija samo ako je prethodno izričito izrazio svoj izbor, ovisno o slučaju, na temelju informiranog individualnog podešavanja, da podaci koji se odnose na njega budu javno dostupni neograničenom broju osoba.

Što se općenitije tiče uvjeta za zakonitost obrade osobnih podataka, Sud podsjeća na to da je, na temelju OUZP-a, obrada podataka zakonita samo ako i u onoj mjeri u kojoj je ispitanik dao privolu za obradu svojih osobnih podataka u jednu ili više posebnih svrha[102]. Ako takva privola nije dana uopće ili nije dana dobrovoljno, posebno, informirano i nedvosmisleno, takva je obrada ipak opravdana ako ispunjava jedan od zahtjeva nužnosti[103], koje valja tumačiti usko. Način na koji operator internetske društvene mreže obrađuje osobne podatke može se smatrati nužnim za izvršavanje ugovora u kojemu su ispitanici stranke samo pod uvjetom da je ta obrada objektivno neophodna za ostvarenje svrhe koja je sastavni dio ugovorne činidbe namijenjene tim korisnicima tako da se glavni predmet ugovora ne može ostvariti ako se ne izvrši ta obrada.

Usto, prema mišljenju Suda, obradu podataka o kojoj je riječ može se smatrati nužnom za potrebe legitimnih interesa voditelja obrade ili treće strane samo pod uvjetom da je navedeni operator korisnicima od kojih su prikupljeni podaci naznačio legitimni interes koji se ostvaruje tom obradom, da se ta obrada provodi u granicama onoga što je strogo nužno za ostvarivanje tog legitimnog interesa i da iz odvagivanja suprotstavljenih interesa, s obzirom na sve relevantne okolnosti, proizlazi da interesi ili temeljne slobode

---

100 Na koje se odnosi članak 9. stavak 2. OUZP-a. Ta odredba glasi: „[s]tavak 1. ne primjenjuje se ako je ispunjen[o] jedno od sljedećeg:
(a) ispitanik je dao izričitu privolu za obradu tih osobnih podataka za jednu ili više određenih svrha, osim ako se pravom Unije ili pravom države članice propisuje da ispitanik ne može ukinuti zabranu iz stavka 1.; […]
(e) obrada se odnosi na osobne podatke za koje je očito da ih je objavio ispitanik;
(f) obrada je nužna za uspostavu, ostvarivanje ili obranu pravnih zahtjeva ili kad god sudovi djeluju u sudbenom svojstvu;
[…]".

101 U smislu članka 9. stavka 2. točke (e) OUZP-a

102 U skladu s člankom 6. stavkom 1. prvim podstavkom točkom (a) OUZP-a

103 Koji su navedeni u članku 6. stavku 1. prvom podstavku točkama (b) do (f) OUZP-a. Na temelju tih odredbi obrada je zakonita samo ako i u onoj mjeri u kojoj je, među ostalim, nužna za izvršavanje ugovora u kojem je ispitanik stranka [članak 6. stavak 1. prvi podstavak točka (b) OUZP-a], radi poštovanja pravnih obveza voditelja obrade [članak 6. stavak 1. prvi podstavak točka (c) OUZP-a] ili za potrebe legitimnih interesa voditelja obrade ili treće strane [članak 6. stavak 1. prvi podstavak točka (f) OUZP-a].

i prava tih korisnika ne prevladavaju nad navedenim legitimnim interesom voditelja obrade ili treće strane. Sud je osobito smatrao da, ako navedeni korisnici nisu dali privolu, njihovi interesi i temeljna prava prevladavaju nad interesom operatora internetske društvene mreže za personalizaciju oglašavanja kojom financira svoju aktivnost.

Naposljetku, Sud pobliže određuje da je obrada podataka o kojoj je riječ u glavnom postupku opravdana ako je zaista nužna radi poštovanja pravnih obveza voditelja obrade, na temelju odredbe prava Unije ili prava države članice o kojoj je riječ, ako se tom pravnom osnovom ostvaruje cilj u općem interesu i ta je pravna osnova razmjerna zakonitom cilju koji se želi postići i ako se ta obrada provodi u granicama onoga što je strogo nužno.

Kad je riječ o valjanosti privole korisnika o kojima je riječ za obradu njihovih podataka na temelju OUZP-a, Sud smatra da okolnost da operator internetske društvene mreže ima vladajući položaj na tržištu internetskih društvenih mreža sama po sebi ne sprečava to da korisnici te mreže mogu valjano dati privolu za to da taj operator obrađuje njihove osobne podatke. Međutim, s obzirom na to da ona može utjecati na slobodu izbora tih korisnika i stvoriti jasnu neravnotežu između njih i navedenog operatora, ta okolnost predstavlja važan element za utvrđivanje toga je li privola zaista dana valjano i osobito dobrovoljno, što je dužan dokazati taj operator[104].

Osobito, korisnici društvene mreže o kojima je riječ moraju imati slobodu da u okviru sklapanja ugovora pojedinačno odbiju dati svoju privolu za određene načine obrade koji nisu nužni za izvršavanje ugovora, a da pritom zato ne moraju u cijelosti odustati od uporabe usluge koju nudi operator internetske društvene mreže, što podrazumijeva da navedenim korisnicima bude ponuđena, ovisno o slučaju uz odgovarajuću naknadu, ekvivalentna alternativa koja nije popraćena takvom obradom podataka. Usto, mora se dati zasebna privola za obradu *off* Facebook podataka.

VI. Nacionalna nadzorna tijela

1. Doseg zahtjeva neovisnosti

Presuda od 9. ožujka 2010. (veliko vijeće), Komisija/Njemačka (C-518/07, EU:C:2010:125)

Komisija je Sudu podnijela tužbu radi utvrđenja da je Savezna Republika Njemačka povrijedila obveze koje je bila dužna ispuniti na temelju članka 28. stavka 1. drugog podstavka Direktive 95/46, podvrgavajući državnoj kontroli nadzorna tijela nadležna za

[104] Na temelju članka 7. stavka 1. OUZP-a

nadzor obrade osobnih podataka u privatnom sektoru u različitim saveznim pokrajinama, pogrešno prenoseći na taj način zahtjev „potpune neovisnosti" tijela zaduženih za osiguranje zaštite tih podataka.

Savezna Republika Njemačka tvrdila je da se člankom 28. stavkom 1. drugim podstavkom Direktive 95/46 zahtijeva funkcionalna neovisnost nadzornih tijela, u smislu da ta tijela moraju biti neovisna o privatnom sektoru koji ona nadziru te da ne smiju biti izložena vanjskim utjecajima. Doista, prema njezinu mišljenju, državna kontrola nad njemačkim saveznim pokrajinama nije takav vanjski utjecaj, nego mehanizam unutarnjeg upravnog nadzora koji provode tijela istog upravnog aparata kojeg su dio i nadzorna tijela te su ona obvezna, kao i ta nadzorna tijela, ispunjavati ciljeve Direktive 95/46.

Sud presuđuje da se jamstvom neovisnosti nacionalnih nadzornih tijela, koje je propisano Direktivom 95/46, nastoji osigurati učinkovitost i pouzdanost nadzora poštovanja odredbi u području zaštite fizičkih osoba u pogledu obrade osobnih podataka i treba se tumačiti s obzirom na taj cilj. To jamstvo neovisnosti nije utvrđeno kako bi se tim tijelima i njihovim službenicima dao poseban status, nego radi jačanja zaštite osoba i tijela na koje se odnose njihove odluke pa nadzorna tijela moraju prilikom obavljanja svojih zadaća djelovati objektivno i nepristrano.

Sud smatra da nacionalna nadzorna tijela nadležna za nadzor nad obradom osobnih podataka u privatnom sektoru moraju biti neovisna, što im omogućuje ispunjavanje njihovih zadaća bez vanjskog utjecaja. Ta neovisnost ne isključuje samo svaki utjecaj tijela koja se nadziru, nego i svaki nalog te svaki drugi izravan ili neizravan vanjski utjecaj koji bi mogao dovesti u pitanje izvršavanje zadaća nacionalnih tijela, koje se sastoje u uspostavi pravedne ravnoteže između prava na privatnost i slobodnog kretanja osobnih podataka. Već sama opasnost da bi kontrolna tijela mogla izvršiti politički utjecaj na odluke nadležnih nadzornih tijela dovoljna je da spriječi neovisno obavljanje njihovih zadaća. S jedne strane, mogla bi postojati „prethodna poslušnost" tih nadzornih tijela s obzirom na praksu odlučivanja kontrolnih tijela. S druge strane, budući da nadzorna tijela imaju ulogu zaštitnikâ prava na privatnost, njihove odluke te stoga i ona sama moraju biti izvan bilo kakve sumnje u nepristranost. Dakle, Sud utvrđuje da državna kontrola nad nacionalnim nadzornim tijelima nije usklađena sa zahtjevom neovisnosti.

Presuda od 16. listopada 2012. (veliko vijeće), Komisija/Austrija (C-614/10, EU:C:2012:631)

Komisija je od Suda tužbom zatražila utvrđenje da je Austrija povrijedila obveze koje je bila dužna ispuniti na temelju članka 28. stavka 1. drugog podstavka Direktive 95/46 jer nije poduzela sve potrebne mjere kako bi njezino zakonodavstvo na snazi ispunjavalo kriterij neovisnosti u pogledu Datenschutzkommissiona (Komisija za zaštitu podataka), koji je uspostavljen kao nadzorno tijelo za zaštitu osobnih podataka.

Sud utvrđuje da Austrija nije ispunila svoje obveze smatrajući u biti da kriterij neovisnosti nadzornog tijela ne ispunjava država članica koja uspostavi regulatorni okvir na temelju kojeg je upravni član navedenog tijela državni službenik koji je podvrgnut

kontroli u službi, čiji je ured dio službi nacionalne vlade i u pogledu kojeg predsjednik vlade ima bezuvjetno pravo na obaviještenost o svim aspektima upravljanja navedenim tijelom.

Sud prije svega podsjeća na to da izraz „potpuno neovisno”, koji se nalazi u članku 28. stavku 1. drugom podstavku Direktive 95/46, podrazumijeva da nadzorna tijela moraju uživati neovisnost koja im omogućava obavljanje njihovih zadaća bez vanjskog utjecaja. U tom pogledu za zaštitu nadzornog tijela od svih vanjskih utjecaja nije sama po sebi dostatna činjenica da takvo tijelo ima funkcionalnu neovisnost u smislu da su njegovi članovi neovisni i da ni na koji način nisu vezani uputama u obavljanju svoje dužnosti. Doista, neovisnost koja se u vezi s time zahtijeva ne isključuje samo izravan utjecaj u obliku uputa, nego i neizravan utjecaj koji može usmjeravati odluke nadzornog tijela. Osim toga, budući da nadzorna tijela imaju ulogu zaštitnikâ prava na privatnost, njihove odluke te stoga i ona sama moraju biti izvan bilo kakve sumnje u nepristranost.

Sud pojašnjava da nacionalno nadzorno tijelo ne mora raspolagati posebnom proračunskom stavkom, poput one koja je propisana u članku 43. stavku 3. Uredbe br. 45/2001, kako bi se mogao ispuniti kriterij neovisnosti iz gore navedene odredbe Direktive 95/46. Naime, države članice nisu obvezne preuzeti u svoje nacionalno zakonodavstvo odredbe istovjetne onima poglavlja V. Uredbe br. 45/2001 kako bi se zajamčila potpuna neovisnost njihova jednog ili više nadzornih tijela pa one, dakle, mogu propisati da nadzorno tijelo proračunski ovisi o određenom ministarstvu. Međutim, dodjela ljudskih i materijalnih resursa koji su mu potrebni ne smije sprečavati takvo tijelo u „potpuno neovisnom” obavljanju njegovih zadaća u smislu članka 28. stavka 1. drugog podstavka Direktive 95/46.

Presuda od 8. travnja 2014. (veliko vijeće), Komisija/Mađarska (C-288/12, EU:C:2014:237)

Komisija je u tom predmetu zatražila od Suda da utvrdi da je Mađarska povrijedila svoje obveze koje je bila dužna ispuniti na temelju Direktive 95/46 jer je prijevremeno okončala mandat nadzornog tijela za zaštitu osobnih podataka.

Sud presuđuje da država članica koja prijevremeno okonča mandat nadzornog tijela za zaštitu osobnih podataka povređuje obveze koje je dužna ispuniti na temelju Direktive 95/46.

Naime, Sud navodi da neovisnost koju moraju uživati nadzorna tijela nadležna za nadzor nad obradom navedenih podataka isključuje svaki nalog te svaki drugi izravan ili neizravan vanjski utjecaj koji bi mogao usmjeriti njihove odluke i koji bi također mogao dovesti u pitanje izvršavanje zadaća nacionalnih tijela, a koje se sastoje u uspostavi pravedne ravnoteže između prava na privatnost i slobodnog kretanja osobnih podataka.

Usto, Sud podsjeća na to da za zaštitu nadzornog tijela od svih vanjskih utjecaja nije sama po sebi dostatna funkcionalna neovisnost jer je sama opasnost da državna kontrolna tijela mogu izvršiti politički utjecaj na odluke nadzornih tijela dovoljna da ih spriječi u neovisnom obavljanju zadaća. Doista, kad bi svaka država članica mogla

okončati mandat nadzornog tijela prije isteka roka koji je za to prvotno predviđen, bez poštovanja pravila i jamstava koja su unaprijed utvrđena u tu svrhu primjenjivim propisom, prijetnja takvog prijevremenog prestanka koja bi postojala za to nacionalno tijelo tijekom izvršavanja njegova mandata mogla bi dovesti do određenog oblika poslušnosti tog tijela političkoj vlasti, koja bi bila nespojiva s navedenim zahtjevom neovisnosti. Štoviše, u takvoj se situaciji ne može smatrati da nadzorno tijelo djeluje u svim okolnostima izvan svake sumnje u njegovu nepristranost.

2. Određivanje primjenjivog prava i nadležnog nadzornog tijela

Presuda od 1. listopada 2015., Weltimmo (C-230/14, EU:C:2015:639)

Nemzeti Adatvédelmi és Információszabadság Hatóság (nacionalno tijelo zaduženo za zaštitu podataka i slobode informiranja, Mađarska) izreklo je novčanu kaznu društvu Weltimmo, koje je bilo registrirano u Slovačkoj te je upravljalo internetskim stranicama za posredovanje nekretninama u Mađarskoj, jer to društvo s tih stranica nije obrisalo osobne podatke oglašivača, iako su oni to zatražili, te je te podatke priopćavalo poduzećima za naplatu potraživanja kako bi naplatilo neplaćene račune. Prema tvrdnjama mađarskog nadzornog tijela, društvo Weltimmo na taj je način povrijedilo mađarski zakon kojim se prenosi Direktiva 95/46.

Postupajući u kasacijskom postupku, Kúria (Vrhovni sud, Mađarska) je izrazila sumnje u vezi s određivanjem primjenjivog prava i u vezi s ovlastima kojima raspolaže mađarsko nadzorno tijelo s obzirom na članak 4. stavak 1. i članak 28. Direktive 95/46. Stoga je Sudu postavila veći broj prethodnih pitanja.

U odnosu na primjenjivo nacionalno pravo Sud presuđuje da članak 4. stavak 1. točka (a) Direktive 95/46 omogućuje primjenu zakonodavstva koje se odnosi na zaštitu osobnih podataka države članice različite od one u kojoj je voditelj obrade tih podataka registriran, ako on putem stabilnih aranžmana na području te države članice obavlja, čak i najmanju, efektivnu i stvarnu djelatnost u okviru koje se ta obrada provodi. Kako bi se utvrdilo je li riječ o takvom slučaju, sud koji je uputio zahtjev može, među ostalim, uzeti u obzir činjenicu, s jedne strane, da se djelatnost voditelja navedene obrade u okviru koje je došlo do te obrade sastoji u upravljanju internetskim stranicama za posredovanje nekretninama koje se odnose na nekretnine smještene na državnom području te države članice i koje su sastavljene na njezinu jeziku te da je ta djelatnost, prema tome, većinom, ako ne i u potpunosti, usmjerena prema navedenoj državi članici. S druge strane, sud koji je uputio zahtjev može uzeti u obzir činjenicu da taj voditelj obrade ima zastupnika u navedenoj državi članici, koji je odgovoran za naplatu potraživanja koja proizlaze iz te djelatnosti kao i za zastupanje u upravnim i sudskim postupcima koji se odnose na obradu predmetnih podataka. Sud, nasuprot tomu, navodi da nije bitno državljanstvo osoba na koje se ta obrada odnosi.

Kad je riječ o nadležnosti i ovlastima nadzornog tijela koje postupa povodom pritužbi u skladu s člankom 28. stavkom 4. Direktive 95/46, Sud smatra da to tijelo može razmatrati

te pritužbe neovisno o primjenjivom pravu i čak i prije nego što dozna koje je nacionalno pravo primjenjivo na predmetnu obradu. Međutim, ako zaključi da je primjenjivo pravo neke druge države članice, ono ne može nametnuti sankcije izvan državnog područja države članice kojoj pripada. U takvoj situaciji na tom je tijelu da, ispunjavajući obvezu suradnje predviđenu člankom 28. stavkom 6. te direktive, od nadzornog tijela te druge države članice zatraži da utvrdi moguću povredu tog prava i nametne sankcije ako to pravo to dopušta, oslanjajući se, prema potrebi, na informacije koje je primilo od tijela prve države članice.

3. Ovlasti nacionalnih nadzornih tijela

Presuda od 6. listopada 2015. (veliko vijeće), Schrems (C-362/14, EU:C:2015:650)

U tom je predmetu (vidjeti također poglavlje IV., naslovljeno „Prijenos osobnih podataka trećim zemljama”) Sud, među ostalim, presudio da su nacionalna nadzorna tijela nadležna za nadzor prijenosa osobnih podataka trećim zemljama.

U tom pogledu Sud prije svega navodi da nacionalna nadzorna tijela raspolažu širokim rasponom ovlasti, indikativno navedenih u članku 28. stavku 3. Direktive 95/46, koje predstavljaju sva nužna sredstva za provedbu njihovih zadaća. Tako navedena tijela imaju, među ostalim, istražne ovlasti, kao što su to ovlasti za prikupljanje svih podataka potrebnih za izvršavanje njihovih nadzornih dužnosti, učinkovite ovlasti za posredovanje, kao što je to nametanje privremene ili konačne zabrane obrade, ili ovlasti za sudjelovanje u sudskim postupcima.

Kad je riječ o ovlasti nadzora prijenosa osobnih podataka u treće zemlje, Sud presuđuje da iz članka 28. stavaka 1. i 6. Direktive 95/46 doista proizlazi da se ovlasti nacionalnih nadzornih tijela odnose na obrade osobnih podataka koje se provode na državnom području države članice u kojoj se nalaze ta tijela, pa stoga na temelju tog članka 28. ne raspolažu ovlastima u pogledu obrada takvih podataka koje su provedene na državnom području treće zemlje.

Međutim, postupak prijenosa osobnih podataka iz države članice u treću zemlju jest kao takav obrada osobnih podataka koja je provedena na državnom području države članice. Posljedično, budući da su nacionalna nadzorna tijela, u skladu s člankom 8. stavkom 3. Povelje i člankom 28. Direktive 95/46, zadužena za nadzor poštovanja pravila Unije o zaštiti fizičkih osoba u vezi s obradom osobnih podataka, svako od tih tijela nadležno je za provjeru poštuje li prijenos tih podataka iz države članice u kojoj se ta tijela nalaze u treću zemlju zahtjeve utvrđene u toj direktivi.

Presuda od 5. lipnja 2018. (veliko vijeće), Wirtschaftsakademie Schleswig-Holstein (C-210/16, EU:C:2018:388)

U toj je presudi (vidjeti također poglavlje II.5., naslovljeno „Pojam ‚voditelj obrade osobnih podataka’”), koja se odnosi, među ostalim, na tumačenje članaka 4. i 28.

Direktive 95/46, Sud odlučivao o opsegu ovlasti za posredovanje kojima nadzorna tijela raspolažu u pogledu obrade osobnih podataka koja podrazumijeva sudjelovanje više sudionika.

Tako Sud presuđuje da, kada poduzetnik sa sjedištem izvan Europske unije (kao što je to društvo Facebook, sa sjedištem u SAD-u) ima nekoliko poslovnih nastana u različitim državama članicama, nadzorno tijelo jedne države članice ima pravo izvršavati ovlasti iz članka 28. stavka 3. te direktive u odnosu na poslovni nastan tog poduzetnika koji se nalazi na državnom području te države članice (u konkretnom slučaju Facebook Germany), iako je, u skladu s raspodjelom zadataka unutar grupe, s jedne strane, taj poslovni nastan odgovoran samo za prodaju oglašivačkog prostora i druge marketinške djelatnosti na državnom području spomenute države članice, dok je, s druge strane, za prikupljanje i obradu osobnih podataka na cijelom području Europske unije isključivo odgovoran poslovni nastan koji se nalazi u drugoj državi članici (u konkretnom slučaju Facebook Ireland).

Usto, Sud pojašnjava da, kada nadzorno tijelo države članice namjerava izvršavati ovlasti za posredovanje iz članka 28. stavka 3. Direktive 95/46 u odnosu na tijelo s poslovnim nastanom na državnom području te države članice zbog povreda pravila o zaštiti osobnih podataka koje je počinila treća osoba odgovorna za obradu tih podataka sa sjedištem u drugoj državi članici (u konkretnom slučaju Facebook Ireland), to je nadzorno tijelo nadležno ocjenjivati zakonitost te obrade neovisno o nadzornom tijelu druge države članice te može izvršavati svoje ovlasti za posredovanje u pogledu tijela s poslovnim nastanom na državnom području te druge države članice (Irske) bez prethodnog pozivanja njezina nadzornog tijela na poduzimanje mjera.

Presuda od 15. lipnja 2021. (veliko vijeće), Facebook Ireland i dr. (C-645/19, EU:C:2021:483)

Predsjednik Commission belge de la protection de la vie privée (belgijska Komisija za zaštitu privatnosti, u daljnjem tekstu: KZP) podnio je protiv društava Facebook Ireland, Facebook Inc. i Facebook Belgium 11. rujna 2015. tužbu za propuštanje pred Nederlandstalige rechtbankom van eerste aanleg Brussel (Prvostupanjski sud na nizozemskom jeziku u Bruxellesu, Belgija), kojom se traži prestanak povreda zakonodavstva u području zaštite podataka koje je navodno počinio Facebook. Te su se povrede sastojale od prikupljanja i uporabe informacija o ponašanju belgijskih korisnika interneta, kako imateljâ računa na Facebooku tako i osoba koje nisu korisnici Facebookovih usluga, putem različitih tehnologija kao što su kolačići, dodaci društvenoj mreži[105] ili pikseli.

Dana 16. veljače 2018. taj se sud proglasio nadležnim za odlučivanje o toj tužbi te je u pogledu merituma presudio da društvena mreža Facebook nije dovoljno obavijestila belgijske korisnike interneta o prikupljanju predmetnih informacija i njihovoj uporabi.

[105] Primjerice gumbi „Sviđa mi se” ili „Podijeli”

Osim toga, pristanak korisnika interneta na prikupljanje i obradu navedenih informacija ocijenjen je nevaljanim.

Dana 2. ožujka 2018. Facebook Ireland, Facebook Inc. i Facebook Belgium protiv te presude uložili su žalbu Hofu van beroep te Brussel (Žalbeni sud u Bruxellesu, Belgija), sudu koji je u ovom predmetu uputio zahtjev za prethodnu odluku. Pred tim sudom tijelo za zaštitu podataka (Belgija) (TZP) djelovalo je kao pravni sljednik predsjednika KZP-a. Sud koji je uputio zahtjev proglasio se nadležnim isključivo za odlučivanje o žalbi koju je podnio Facebook Belgium.

Sud koji je uputio zahtjev iznio je dvojbe u pogledu utjecaja primjene „jedinstvenog mehanizma" predviđenog OUZP-om[106] na nadležnosti TZP-a te je, konkretnije, postavio pitanje može li TZP pokrenuti postupak protiv Facebooka Belgium u odnosu na činjenice nastale nakon stupanja na snagu OUZP-a, odnosno 25. svibnja 2018., s obzirom na to da je kao voditelj obrade predmetnih podataka utvrđen Facebook Ireland. Naime, od tog datuma i osobito na temelju primjene načela „jedinstvenog mehanizma" predviđenog OUZP-om, samo irski Povjerenik za zaštitu podataka nadležan je za podnošenje tužbe za propuštanje, pod nadzorom irskih sudova.

U svojoj presudi, o kojoj je odlučivao u velikom vijeću, Sud precizira ovlasti nacionalnih nadzornih tijela u okviru OUZP-a. On tako, među ostalim, presuđuje da na temelju te uredbe nadzorno tijelo države članice može pod određenim uvjetima izvršavati svoju ovlast obavještavanja suda te države o svakoj navodnoj povredi OUZP-a i pokrenuti postupak u vezi s prekograničnom obradom podataka[107], iako nije vodeće nadzorno tijelo u pogledu te obrade.

Kao prvo, Sud pojašnjava uvjete pod kojima nacionalno nadzorno tijelo koje nije vodeće nadzorno tijelo u pogledu prekogranične obrade mora izvršavati svoju ovlast obavještavanja suda države članice o svakoj navodnoj povredi OUZP-a i, u slučaju potrebe, pokretanja sudskog postupka kako bi se osigurala primjena te uredbe. Tako, s jedne strane, OUZP mora tom nadzornom tijelu dodijeliti ovlast za donošenje odluke kojom se utvrđuje da se tom obradom krše pravila predviđena tom uredbom i, s druge strane, ta se ovlast mora izvršavati uz poštovanje postupaka suradnje i nadzora konzistentnosti predviđenih tom uredbom[108].

Naime, OUZP u odnosu na prekogranične obrade predviđa „jedinstveni mehanizam"[109], koji se temelji na podjeli nadležnosti između „vodećeg nadzornog tijela" i drugih predmetnih nacionalnih nadzornih tijela. Taj mehanizam zahtijeva usku, lojalnu i djelotvornu suradnju između tih tijela, kako bi se osigurala dosljedna i ujednačena primjena pravila o zaštiti osobnih podataka te kako bi se očuvao njihov koristan učinak.

---

[106] U skladu s člankom 56. stavkom 1. OUZP-a: „Ne dovodeći u pitanje članak 55., nadzorno tijelo glavnog poslovnog nastana ili jedinog poslovnog nastana voditelja obrade ili izvršitelja obrade nadležno je djelovati kao vodeće nadzorno tijelo za prekograničnu obradu koju provodi taj voditelj obrade ili izvršitelj obrade u skladu s postupkom utvrđenim u članku 60.".

[107] U smislu članka 4. točke 23. OUZP-a

[108] Predviđenih člancima 56. i 60. OUZP-a

[109] Članak 56. stavak 1. OUZP-a

OUZP u tom pogledu propisuje načelnu nadležnost vodećeg nadzornog tijela za donošenje odluke kojom se utvrđuje da se prekograničnom obradom krše pravila predviđena tom uredbom[110], dok je nadležnost drugih nacionalnih nadzornih tijela za donošenje takve odluke, makar i privremeno, iznimka[111]. Međutim, vodeće nadzorno tijelo prilikom izvršavanja svojih nadležnosti ne može zanemariti potreban dijalog te lojalnu i djelotvornu suradnju s drugim predmetnim nadzornim tijelima. Posljedično tomu, u okviru te suradnje, vodeće nadzorno tijelo ne može zanemariti stajališta drugih predmetnih nadzornih tijela, a svaki relevantan i obrazložen prigovor koji jedno od tih tijela iznese rezultira, barem privremeno, blokiranjem donošenja nacrta odluke vodećeg nadzornog tijela.

Sud nadalje pojašnjava da je okolnost da nadzorno tijelo države članice koje nije vodeće nadzorno tijelo kad je riječ o prekograničnoj obradi podataka može izvršavati ovlast obavještavanja suda te države o svakoj navodnoj povredi OUZP-a i pokretanja sudskog postupka samo uz poštovanje pravila o podjeli nadležnosti za odlučivanje između vodećeg nadzornog tijela i drugih nadzornih tijela[112] u skladu s člancima 7., 8. i 47. Povelje, kojima se dotičnoj osobi jamči pravo na zaštitu njezinih osobnih podataka i pravo na djelotvoran pravni lijek.

Kao drugo, Sud presuđuje da u slučaju prekogranične obrade podataka izvršavanje ovlasti nadzornog tijela države članice koje nije vodeće nadzorno tijelo da pokrene sudski postupak[113] ne zahtijeva da voditelj ili izvršitelj prekogranične obrade osobnih podataka protiv kojeg je pokrenut taj postupak ima glavni poslovni nastan ili drugi poslovni nastan na području te države članice. Međutim, izvršavanje te ovlasti mora biti obuhvaćeno teritorijalnim područjem primjene OUZP-a[114], što znači da voditelj ili izvršitelj prekogranične obrade ima poslovni nastan na području Unije.

Kao treće, Sud odlučuje da se u slučaju prekogranične obrade podataka ovlast nadzornog tijela države članice koje nije vodeće nadzorno tijelo da o svakoj navodnoj povredi OUZP-a obavijesti sud te države i, u slučaju potrebe, pokrene sudski postupak, može izvršavati kako u odnosu na glavni poslovni nastan voditelja obrade koji se nalazi u državi članici tog tijela tako i u odnosu na drugi poslovni nastan tog voditelja, pod uvjetom da se sudski postupak odnosi na obradu podataka izvršenu u okviru aktivnosti tog poslovnog nastana i da je navedeno tijelo nadležno za izvršavanje te ovlasti.

Ipak, Sud ističe da izvršavanje te ovlasti podrazumijeva da je OUZP primjenjiv. U predmetnom slučaju, s obzirom na to da su aktivnosti poslovnog nastana grupe Facebook u Belgiji neodvojivo povezane s obradom osobnih podataka o kojoj je riječ u glavnom postupku, za koju je na području Unije odgovoran Facebook Ireland, ta se

110 Članak 60. stavak 7. OUZP-a

111 Članak 56. stavak 2. i članak 66. OUZP-a propisuju iznimke od načela nadležnosti za odlučivanje vodećeg nadzornog tijela.

112 Predviđenih člancima 55. i 56., u vezi s člankom 60. OUZP-a

113 Na temelju članka 58. stavka 5. OUZP-a

114 Člankom 3. stavkom 1. OUZP-a predviđa se da se ta uredba primjenjuje na obradu osobnih podataka „u okviru aktivnosti poslovnog nastana voditelja obrade ili izvršitelja obrade u Uniji, neovisno o tome obavlja li se obrada u Uniji ili ne”.

obrada izvršava „u okviru aktivnosti poslovnog nastana voditelja obrade” i stoga je doista obuhvaćena područjem primjene OUZP-a.

Kao četvrto, Sud presuđuje da, kad je nadzorno tijelo države članice koje nije „vodeće nadzorno tijelo” pokrenulo sudski postupak u pogledu prekogranične obrade osobnih podataka prije datuma stupanja na snagu OUZP-a, navedeni postupak može se, u skladu s pravom Unije, nastaviti na temelju odredbi Direktive 95/46 koja se i dalje primjenjuje u pogledu povreda u njoj predviđenih pravila počinjenih do datuma kad je ta direktiva stavljena izvan snage. Nadalje, navedeni postupak to tijelo može pokrenuti za povrede počinjene nakon stupanja na snagu OUZP-a, pod uvjetom da se radi o jednoj od situacija u kojima ta uredba iznimno dodjeljuje tom tijelu nadležnost za donošenje odluke kojom se utvrđuje da se predmetnom obradom podataka povređuju pravila iz te uredbe te uz poštovanje u njoj predviđenih postupaka suradnje i nadzora konzistentnosti.

Kao peto i posljednje, Sud priznaje izravan učinak odredbe OUZP-a na temelju koje svaka država članica zakonom propisuje da je njezino nadzorno tijelo ovlašteno obavijestiti sudove o svakoj povredi te uredbe i, u slučaju potrebe, pokrenuti sudski postupak. Posljedično tomu, takvo tijelo može se pozvati na tu odredbu kako bi pokrenulo ili nastavilo postupak protiv pojedinaca, čak i ako navedena odredba nije posebno provedena u zakonodavstvu predmetne države članice.

Presuda od 16. siječnja 2024. (veliko vijeće), Österreichische Datenschutzbehörde (C-33/22, EU:C:2024:46)

U tom predmetu (vidjeti također poglavlje II.1., naslovljeno „Područje primjene općih propisa”), Sud ističe da odredbe OUZP-a o nadležnosti nacionalnih nadzornih tijela i pravu na pritužbu[115] ne zahtijevaju donošenje nacionalnih provedbenih mjera te da su dovoljno jasne, precizne i bezuvjetne kako bi imale izravan učinak. Iz toga slijedi da, iako je OUZP-om državama članicama priznata margina prosudbe u pogledu broja nadzornih tijela koja treba uspostaviti [116], njime se, naprotiv, utvrđuje opseg njihove nadležnosti za praćenje primjene te uredbe. Stoga, u slučaju da država članica odluči osnovati samo jedno nadzorno tijelo, ono nužno ima sve ovlasti koje su predviđene OUZP-om. Svakim suprotnim tumačenjem bio bi doveden u pitanje koristan učinak tih odredbi te bi se riskiralo slabljenje korisnog učinka svih drugih odredbi OUZP-a na koje bi se pritužba mogla odnositi.

Što se tiče okolnosti da se nacionalnim ustavnopravnim odredbama isključuje mogućnost da nadzorno tijelo koje ovisi o izvršnoj vlasti nadzire način na koji OUZP primjenjuje tijelo koje je dio zakonodavne vlasti, Sud naglašava da se OUZP-om od država članica zahtijeva, poštujući upravo njihovu ustavnu strukturu, samo da uspostave barem jedno nadzorno tijelo, pri čemu im se nudi mogućnost da uspostave više njih. Stoga se tom uredbom svakoj državi članici priznaje margina prosudbe koja joj

[115] Članak 55. stavak 1. odnosno članak 77. stavak 1. OUZP-a
[116] U skladu s člankom 51. stavkom 1. OUZP-a

omogućuje uspostavu onoliko nadzornih tijela koliko je to potrebno s obzirom na, među ostalim, zahtjeve koji se odnose na njezinu ustavnu strukturu.

Usto, pozivanje države članice na odredbe nacionalnog prava ne može ugroziti jedinstvo i učinkovitost prava Unije. Naime, učinci načela nadređenosti prava Unije obvezuju sva tijela države članice, pri čemu tomu ne mogu biti prepreka, među ostalim, nacionalne odredbe, uključujući one ustavne prirode.

Stoga, ako je država članica odlučila uspostaviti samo jedno nadzorno tijelo, ona se ne može pozivati na odredbe nacionalnog prava, pa bile one i ustavne prirode, kako bi obradu osobnih podataka koja je obuhvaćena područjem primjene OUZP-a izuzela od praćenja tog tijela.

4. Uvjeti za izricanje upravnih novčanih kazni

Presuda od 5. prosinca 2023. (veliko vijeće), Nacionalinis visuomenės sveikatos centras (C-683/21, EU:C:2023:949)

U tom predmetu (vidjeti također poglavlja II.3., II.5. i II.6., naslovljena „ Pojam ‚obrada osobnih podataka'", „Pojam ‚voditelj obrade osobnih podataka'" i „Pojam ‚zajednički voditelj obrade'") Sud je utvrdio da se na temelju članka 83. OUZP-a voditelju obrade može izreći upravna novčana kazna samo ako se utvrdi da je namjerom ili nepažnjom prekršio pravila sadržana u toj uredbi[117].

U tom pogledu Sud pojašnjava da zakonodavac Unije nije državama članicama ostavio marginu prosudbe u pogledu materijalnih uvjeta koje nadzorno tijelo mora poštovati kada odluči izreći upravnu novčanu kaznu voditelju obrade na temelju te odredbe. Činjenica da se OUZP-om državama članicama daje mogućnost da predvide iznimke u odnosu na tijela javne vlasti i javna tijela sa sjedištem na njihovu državnom području[118] kao i zahtjeve koji se odnose na postupak koji nadzorna tijela moraju slijediti za izricanje upravne novčane kazne[119] nipošto ne znači da su te države također ovlaštene predvidjeti takve materijalne uvjete.

Što se tiče tih uvjeta, Sud napominje da se među elementima navedenima u OUZP-u, na temelju kojih nadzorno tijelo voditelju obrade izriče administrativnu novčanu kaznu, nalazi „činjenica da je povreda počinjena namjerno ili nepažnjom"[120]. Nasuprot tomu, nijedan od tih elemenata ne upućuje ni na kakvu mogućnost utvrđivanja odgovornosti voditelja obrade ako nije postojalo njegovo skrivljeno postupanje. Stoga samo povrede

[117] Kršenje iz članka 83. stavaka 4. do 6.

[118] Na temelju članka 83. stavka 7. OUZP-a kojim se predviđa da „[...] svaka država članica može utvrditi pravila mogu li se i u kojoj mjeri tijelima javne vlasti i javnim tijelima osnovanima u toj državi članici izreći upravne novčane kazne".

[119] Na temelju članka 83. stavka 8. OUZP-a, u vezi s njegovom uvodnom izjavom 129.

[120] Članak 83. stavak 2. točka (b) OUZP-a.

odredbi OUZP-a koje je voditelj obrade počinio namjerno ili nepažnjom mogu dovesti do toga da mu se izrekne upravna novčana kazna u skladu s člankom 83. te uredbe.

Sud dodaje da je to tumačenje potkrijepljeno općom strukturom i svrhom OUZP-a. U tom kontekstu pojašnjava je da postojanje sustava sankcija na temelju OUZP-a, koji omogućuje da se, kada to opravdavaju posebne okolnosti svakog pojedinog slučaja, izrekne upravna novčana kazna, potiče voditelje obrade i izvršitelje obrade da postupaju u skladu s tom uredbom i da upravne novčane kazne svojim odvraćajućim učinkom pridonose jačanju zaštite ispitanika. Međutim, zakonodavac Unije nije smatrao potrebnim predvidjeti izricanje upravnih novčanih kazni ako ne postoji krivnja. Uzimajući u obzir činjenicu da OUZP ima za cilj razinu zaštite koja je i jednaka i homogena i da se u tu svrhu mora dosljedno primjenjivati u cijeloj Uniji, bilo bi protivno toj svrsi dopustiti državama članicama da predvide takav sustav za izricanje novčane kazne.

Osim toga, Sud zaključuje da se takva novčana kazna može izreći voditelju obrade za postupke obrade osobnih podataka koje provodi izvršitelj obrade u njegovo ime, osim ako je u okviru tih postupaka taj izvršitelj obrade izvršio obradu u vlastite svrhe ili je te podatke obradio na način koji nije u skladu s okvirom ili sredstvima obrade kako ih je odredio voditelj obrade ili na način da se ne može razumno smatrati da je taj voditelj obrade na to pristao. U tom slučaju izvršitelj obrade se treba smatrati voditeljem takve obrade.

Presuda od 5. prosinca 2023. (veliko vijeće), Deutsche Wohnen (C-807/21, EU:C:2023:950)

Deutsche Wohnen SE (u daljnjem tekstu: DW) društvo je za poslovanje nekretninama koje neizravno, preko udjela u različitim društvima, raspolaže mnogobrojnim poslovnim i stambenim jedinicama. U okviru svojih poslovnih djelatnosti obrađuje osobne podatke zakupoprimaca i najmoprimaca tih jedinica.

Nakon dviju kontrola provedenih 2017. i 2019., Berliner Beauftragte für den Datenschutz (službenik za zaštitu podataka u Berlinu, Njemačka) utvrdio je niz kršenja OUZP-a koja je počinio DW. Odlukom od 30. listopada 2019. taj mu je službenik za zaštitu podataka u tom pogledu izrekao upravne novčane kazne.

DW je podnio tužbu protiv te odluke Landgerichtu Berlin (Zemaljski sud u Berlinu, Njemačka), koji je obustavio postupak. Taj je sud istaknuo da se na temelju njemačkog prava[121] upravni prekršaj može utvrditi samo protiv fizičke osobe, a ne protiv pravne osobe. Osim toga, u slučaju utvrđivanja odgovornosti pravne osobe mogu joj se pripisati samo akti članova njezinih tijela ili njezinih zastupnika. Staatsanwaltschaft Berlin (Državno odvjetništvo u Berlinu, Njemačka) podnio je žalbu protiv te odluke Kammergerichtu Berlin (Visoki zemaljski sud u Berlinu, Njemačka). U tom je kontekstu taj sud uputio Sudu zahtjev za prethodnu odluku o tumačenju OUZP-a.

[121] Gesetz über Ordnungswidrigkeiten (Zakon o upravnim prekršajima) od 24. svibnja 1968. (BGBl. 1968. I, str. 481.), u verziji prema Obavijesti od 19. veljače 1987. (BGBl. 1987. I, str. 602.), kako je prilagođen Zakonom od 19. lipnja 2020. (BGBl. 2020. I, str. 1350.)

Sud, zasjedajući u velikom vijeću, u svojoj presudi odlučuje o uvjetima izricanja upravnih novčanih kazni na temelju OUZP-a. Kao prvo, sud koji je uputio zahtjev ispituje mogu li države članice izricanje upravne novčane kazne pravnoj osobi uvjetovati time da se kršenje te uredbe prethodno pripiše identificiranoj fizičkoj osobi. Kao drugo, također se bavi, kao i u presudi Nacionalinis visuomenės sveikatos centras (vidjeti *supra*) pitanjem treba li sankcionirano kršenje odredbi OUZP-a biti počinjeno namjerno ili nepažnjom.

Što se tiče izricanja upravne novčane kazne na temelju OUZP-a pravnoj osobi, Sud najprije ističe da se načela, zabrane i obveze predviđene OUZP-om osobito odnose na „voditelje obrade" čija se odgovornost proteže na svaku obradu osobnih podataka koju sami provode ili koja se provodi u njihovo ime. Ta je odgovornost, u slučaju kršenja odredbi OUZP-a, temelj za izricanje upravne novčane kazne voditelju obrade u skladu s člankom 83. te uredbe. Međutim, zakonodavac Unije u svrhu utvrđivanja takve odgovornosti nije napravio razliku između fizičkih i pravnih osoba jer je ta odgovornost uvjetovana samo time da one same ili zajedno s drugima određuju svrhe i sredstva obrade osobnih podataka[122]. Stoga je u načelu svaka osoba koja ispunjava taj uvjet osobito odgovorna za svako kršenje OUZP-a koje počini sama ili koje je počinjeno u njezino ime. To znači, s jedne strane, da su pravne osobe odgovorne za kršenja koja su počinili ne samo njihovi zastupnici, direktori ili rukovoditelji nego i sve druge osobe koje djeluju u okviru poslovne aktivnosti tih pravnih osoba i u njihovo ime. S druge strane, upravne novčane kazne predviđene OUZP-om u slučaju takvih kršenja moraju se moći izravno izreći pravnim osobama ako se mogu smatrati voditeljima obrade.

Nadalje, Sud primjećuje da nijedna odredba OUZP-a ne omogućuje zaključak da izricanje upravne novčane kazne pravnoj osobi kao voditelju obrade podliježe prethodnom utvrđenju da je to kršenje počinila identificirana fizička osoba. Osim toga, zakonodavac Unije nije državama članicama ostavio marginu prosudbe u tom pogledu. Činjenica da im OUZP daje mogućnost da predvide zahtjeve u pogledu postupka koji nadzorna tijela trebaju slijediti radi izricanja upravne novčane kazne[123] nipošto ne znači da su također ovlaštene predvidjeti dodatne materijalne uvjete uz one određene OUZP-om.

U tom kontekstu Sud pojašnjava da bi dopustiti državama članicama da jednostrano i kao nužan uvjet za izricanje upravne novčane kazne u skladu s člankom 83. OUZP-a voditelju obrade koji je pravna osoba zahtijevaju da se predmetno kršenje prethodno pripiše ili da se prethodno može pripisati identificiranoj fizičkoj osobi bilo protivno svrsi OUZP-a. Usto, takav bi dodatni zahtjev u konačnici mogao oslabiti djelotvornost i odvraćajući učinak upravnih novčanih kazni izrečenih pravnim osobama kao voditeljima obrade.

Naposljetku, Sud naglašava da pojam „poduzetnik", u smislu članaka 101. i 102. UFEU-a[124], ne utječe na pitanje može li se i pod kojim uvjetima voditelju obrade koji je

[122] U skladu s člankom 4. točkom 7. OUZP-a

[123] Kao što to proizlazi iz članka 58. stavka 4. i članka 83. stavka 8. OUZP-a, u vezi s njegovom uvodnom izjavom 129.

[124] Na koji se upućuje u uvodnoj izjavi 150. OUZP-a

pravna osoba izreći upravna novčana kazna u skladu s OUZP-om te je relevantan samo za određivanje iznosa takve novčane kazne.

Stoga Sud zaključuje da se OUZP-u[125] protivi nacionalni propis na temelju kojeg se pravnoj osobi u svojstvu voditelja obrade može izreći upravna novčana kazna za kršenje te uredbe[126] samo ako je to kršenje prethodno pripisano identificiranoj fizičkoj osobi.

Što se tiče pitanja mogu li države članice predvidjeti izricanje upravne novčane kazne čak i ako sankcionirano kršenje nije počinjeno namjerno ili nepažnjom, Sud najprije podsjeća na to da su materijalni uvjeti koje nadzorno tijelo mora poštovati kada izriče upravnu novčanu kaznu voditelju obrade obuhvaćeni samo pravom Unije i da države članice u tom pogledu nemaju nikakvi manevarski prostor. Slijedeći rasuđivanje istovjetno onomu u gore navedenoj presudi Nacionalinis visuomenės sveikatos centras, Sud utvrđuje da se na temelju članka 83. OUZP-a upravna novčana kazna može izreći samo ako se dokaže da je voditelj obrade, koji je istodobno pravna osoba i poduzetnik, namjerno ili nepažnjom prekršio pravila sadržana u toj uredbi.

5. Odnos između nadležnosti nacionalnih nadzornih tijela i nadležnosti drugih nacionalnih tijela

Presuda od 4. srpnja 2023. (veliko vijeće), Meta Platforms i dr. (Opći uvjeti uporabe društvene mreže) (C-252/21, EU:C:2023:537)

U tom predmetu (vidjeti također poglavlje V.5., naslovljeno „Obrada osobnih podataka na internetskim društvenim mrežama”), odlučujući o ovlasti tijela nadležnog za tržišno natjecanje za utvrđivanje neusklađenosti obrade osobnih podataka s OUZP-om, Sud utvrđuje da, pod uvjetom da tijelo države članice nadležno za tržišno natjecanje poštuje svoju obvezu lojalne suradnje[127] s nadzornim tijelima, ono može utvrditi, u okviru ispitivanja zlouporabe vladajućeg položaja poduzetnika[128], da opći uvjeti uporabe tog poduzetnika koji se odnose na obradu osobnih podataka i njihova provedba nisu usklađeni s tom uredbom, ako je to utvrđenje nužno za dokazivanje postojanja takve zlouporabe. Međutim, kada tijelo nadležno za tržišno natjecanje utvrdi povredu OUZP-a u okviru utvrđenja zlouporabe vladajućeg položaja, ono ne zamjenjuje nadzorna tijela.

Stoga, uzimajući u obzir načelo lojalne suradnje, kada su nacionalna tijela nadležna za tržišno natjecanje prilikom izvršavanja svojih nadležnosti dužna ispitati usklađenost postupanja određenog poduzetnika s odredbama OUZP-a, ona se moraju uskladiti i lojalno surađivati s nacionalnim nadzornim tijelima o kojima je riječ ili s vodećim

[125] Članak 58. stavak 2. točka (i) i članak 83. stavci 1. do 6. OUZP-a
[126] Iz članka 83. stavaka 4. do 6. OUZP-a
[127] Sadržanog u članku 4. stavku 3. UEU-a
[128] U smislu članka 102. UFEU-a

nadzornim tijelom. Sva su ta tijela stoga dužna poštovati svoje ovlasti i nadležnosti kako bi se poštovale obveze koje proizlaze iz OUZP-a i ciljevi te uredbe i kako bi se očuvao njihov korisni učinak. Iz toga slijedi da, kada, u okviru ispitivanja čiji je cilj utvrditi postojanje zlouporabe vladajućeg položaja određenog poduzetnika, nacionalno tijelo nadležno za tržišno natjecanje smatra da je nužno ispitati usklađenost postupanja tog poduzetnika s obzirom na odredbe OUZP-a, navedeno tijelo mora provjeriti jesu li u pogledu tog postupanja ili sličnog postupanja nadležno nacionalno nadzorno tijelo ili vodeće nadzorno tijelo ili pak Sud već donijeli odluku. Ako to jest tako, nacionalno tijelo nadležno za tržišno natjecanje ne može odstupiti od nje, ali ostaje slobodno da iz nje izvuče vlastite zaključke iz perspektive primjene prava tržišnog natjecanja.

Kada dvoji o dosegu ocjene koju provodi nadležno nacionalno nadzorno tijelo ili vodeće nadzorno tijelo, kada u pogledu postupanja o kojem je riječ ili sličnog postupanja ta tijela istodobno provode ispitivanje ili pak kada, ako navedena tijela nisu provela istragu, ono smatra da poduzetnikovo postupanje nije usklađeno s odredbama OUZP-a, nacionalno tijelo nadležno za tržišno natjecanje mora se obratiti tim tijelima i od njih zahtijevati njihovu suradnju kako bi otklonilo te dvojbe ili odredilo treba li čekati da nadležno tijelo o kojem je riječ donese odluku prije nego što započne vlastito ocjenjivanje. Ako ta tijela ne prigovore ni ne odgovore u razumnom roku, tijelo nadležno za tržišno natjecanje može provesti vlastitu istragu.

SUD
EUROPSKE UNIJE

Uprava za istraživanje i dokumentaciju

Srpanj 2024.