Preporuke

Preporuke 02/2020 o europskim temeljnim jamstvima za mjere nadzora

Doneseno 10. studenoga 2020.

Translations proofread by EDPB Members.
This language version has not yet been proofread.

Sadržaj

1. UVOD 4
2. ZADIRANJA U TEMELJNA PRAVA 6
3. EUROPSKA TEMELJNA JAMSTVA 8
Jamstvo A – Obrada bi se trebala temeljiti na jasnim, preciznim i pristupačnim pravilima 8
Jamstvo B – Nužnost i proporcionalnost u pogledu legitimnih ciljeva koji se žele postići moraju se dokazati 10
Jamstvo C – Neovisan nadzorni sustav 12
Jamstvo D – Učinkoviti pravni lijekovi trebaju biti dostupni pojedincu 13
4. ZAVRŠNE NAPOMENE 14

Europski odbor za zaštitu podataka

uzimajući u obzir članak 70. stavak 1. točku (e) Uredbe 2016/679/EU 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, (u daljnjem tekstu: Opća uredba),[1]

uzimajući u obzir Sporazum o Europskom gospodarskom prostoru, a posebno njegov Prilog XI. i Protokol 37., kako su izmijenjeni Odlukom Zajedničkog odbora EGP-a br. 154/2018 od 6. srpnja 2018.[2],

uzimajući u obzir članak 12. i članak 22. svojeg Poslovnika,

uzimajući u obzir članak 29. radnog dokumenta Radne skupine o opravdanosti zadiranja u temeljna prava na privatnost i zaštitu podataka kroz nadzorne mjere tijekom prijenosa osobnih podataka (europska temeljna jamstva, u daljnjem tekstu: ETJ), WP237,

DONIO JE SLJEDEĆE PREPORUKE

1. UVOD

1. Nakon presude Schrems I, tijela EU-a za zaštitu podataka okupljena u Radnoj skupini 29 oslonila su se na sudsku praksu kako bi utvrdila europska temeljna jamstva koja je potrebno poštovati kako bi se osiguralo da u demokratskom društvu zadiranje u prava na privatnost i zaštitu osobnih podataka, s pomoću mjera nadzora i tijekom prijenosa osobnih podataka, ne prelazi ono što je nužno i proporcionalno.

2. Europski odbor za zaštitu podataka želi naglasiti da se europska temeljna jamstva temelje na sudskoj praksi Suda Europske unije (u daljnjem tekstu: Sud EU-a) povezanoj s člancima 7., 8., 47. i 52. Povelje Europske unije o temeljnim pravima (u daljnjem tekstu Povelja) i, ovisno o slučaju, o sudskoj praksi Europskog suda za ljudska prava (u daljnjem tekstu: ESLJP) povezanoj s člankom 8. Europske konvencija o ljudskim pravima (u daljnjem tekstu: EKLJP) koja se bavi rješavanjem pitanja nadzora u državama članicama EKLJP-a.[3]

[1] Ovaj se rad ne odnosi na slučajeve prijenosa ili daljnje razmjene koji su obuhvaćeni područjem primjene Direktive za provedbu zakona (Direktiva (EU) 2016/680).

[2] Upućivanja na „države članice" u ovom dokumentu trebala bi se tumačiti kao upućivanja na „države članice EGP-a".

[3] U tim Preporukama pojam „temeljna prava" proizlazi iz Povelje EU-a o temeljnim pravima. Međutim, koristi se i za obuhvaćanje „ljudskih prava" kako su uključena u Europsku konvenciju o ljudskim pravima.

3. Svrha je ažuriranja ovog dokumenta dodatno razviti europska temeljna jamstva, izvorno sastavljena kao odgovor na presudu Schrems I,[4] odražavajući razjašnjenja koja je dao Sud Europske unije (i Europski sud za ljudska prava) od njegova prvog objavljivanja, posebno u svojoj važnoj presudi Schrems II.[5]

4. U svojoj presudi Schrems II, Sud Europske unije naveo je da ispitivanjem Odluke Komisije 2010/87/EU o standardnim ugovornim klauzulama za prijenos osobnih podataka obrađivačima s poslovnim nastanom u trećim zemljama, s obzirom na članke 7., 8. i 47. Povelje, nije otkriveno ništa što bi utjecalo na valjanost te odluke, već je poništena Odluka o sustavu zaštite privatnosti. Sud Europske unije smatrao je da Odluka o sustavu zaštite privatnosti nije spojiva s člankom 45. stavkom 1. Opće uredbe, s obzirom na članke 7., 8. i 47. Povelje. Presuda stoga može poslužiti kao primjer ako mjere nadzora u trećoj zemlji (u ovom slučaju SAD s odjeljkom 702. FISA-e i izvršnim nalogom 12 333) nisu dovoljno ograničene niti su predmet učinkovite sudske zaštite dostupne ispitanicima za ostvarivanje njihovih prava, kako je propisano pravom Unije, kako bi se razina zaštite u trećoj zemlji smatrala „bitno istovjetnom" onoj zajamčenoj u Europskoj uniji u smislu članka 45. stavka 1. Opće uredbe.

5. Razlozi za proglašenje ništavosti zaštite privatnosti imaju posljedice i na druge alate za prijenos[6]. Iako je Sud tumačio članak 46. stavak 1. Opće uredbe u kontekstu valjanosti standardnih ugovornih klauzula (u daljnjem tekstu: (SUK-ovi), njihovo se tumačenje primjenjuje na svaki prijenos u treće zemlje koji se oslanja na bilo koji od alata iz članka 46. Opće uredbe.[7]

6. Sud EU-a u konačnici prosuđuje mogu li zadiranja u temeljna prava biti opravdana. Međutim, u nedostatku takve presude i u primjeni stalne sudske prakse, tijela za zaštitu podataka dužna su procijeniti pojedinačne predmete, bilo po službenoj dužnosti ili nakon žalbe, i uputiti predmet nacionalnom sudu ako sumnjaju da prijenos nije u skladu s člankom 45. kada postoji odluka o prikladnosti, ili suspendirati ili zabraniti prijenos ako utvrde da se članak 46. Opće uredbe ne može poštovati, a zaštita prenesenih podataka koja se zahtijeva pravom Unije ne može biti zajamčena drugim sredstvima.

7. Cilj ažuriranih europskih temeljnih jamstava jest pružiti elemente kojima će se ispitati mogu li se mjere nadzora kojima se javnim tijelima u trećoj zemlji omogućuje pristup osobnim podatcima, kao nacionalnim sigurnosnim agencijama ili tijelima kaznenog progona, smatrati opravdanim zadiranjem ili ne.

8. Naime, europska temeljna jamstva dio su procjene koju treba provesti kako bi se utvrdilo pruža li treća zemlja razinu zaštite koja je bitno istovjetna onoj zajamčenoj unutar EU-a, ali sama po sebi nisu namijenjena utvrđivanju svih elemenata koji su potrebni kako bi se moglo smatrati da treća zemlja pruža takvu razinu zaštite u skladu s člankom 45. Opće uredbe. Također, ona nemaju za cilj samostalno utvrđivanje svih elemenata koje je možda potrebno uzeti u obzir tijekom procjene sprječava li pravni poredak treće zemlje izvoznika podataka i uvoznika podataka da osiguraju odgovarajuće zaštitne mjere u skladu s člankom 46. Opće uredbe.

[4] Presuda Suda Europske unije od 6. listopada 2015., Maximillian Schrems protiv povjerenika za zaštitu podataka, predmet C-362/14, EU:C:2015:650 (u daljnjem tekstu: „Schrems I").

[5] Presuda Suda Europske unije od 16. srpnja 2020., Povjerenik za zaštitu podataka protiv Facebook Ireland Ltd. i Maximillian Schrems, predmet C-311/18, ECLI:EU:C:2020:559 (u daljnjem tekstu: Schrems II).

[6] Vidjeti t. 105. presude Schrems II.

[7] Vidjeti t. 92. presude Schrems II.

9. Stoga bi se elementi navedeni u ovom radu trebali smatrati temeljnim jamstvima koja treba pronaći u trećoj zemlji tijekom procjene zadiranja, koji proizlaze iz mjera nadzora treće zemlje, s pravima na privatnost i zaštitu podataka, a ne popisom elemenata kojima se dokazuje da pravni režim treće zemlje pruža bitno istovjetnu razinu zaštite.

10. Člankom 6. stavkom 3. Ugovora o Europskoj uniji utvrđeno je da temeljna prava sadržana u EKLJP-u čine opća načela prava Unije. Međutim, kako Sud podsjeća u svojoj sudskoj praksi, ona ne predstavlja, sve dok joj Europska unija nije pristupila, pravni instrument koji je formalno uključen u pravo Unije.[8] Stoga se razina zaštite temeljnih prava potrebna prema članku 46. stavku 1. Opće uredbe mora utvrditi na temelju odredbi te Uredbe, u smislu temeljnih prava sadržanih u Povelji. S obzirom na navedeno, u skladu s člankom 52. stavkom 3. Povelje, prava sadržana u Povelji koja odgovaraju pravima zajamčenima EKLJP-om moraju imati isto značenje i područje primjene kao ona utvrđena tom Konvencijom i slijedom toga, kao što upozorava Sud Europske unije, mora se uzeti u obzir sudska praksa ESLJP-a u pogledu prava koja su također predviđena Poveljom o temeljnim pravima EU-a, kao minimalni prag zaštite za tumačenje odgovarajućih prava iz Povelje[9]. Međutim, u skladu s posljednjom rečenicom članka 52. stavka 3. Povelje, „ova odredba ne sprječava pravo Unije da pruži širu zaštitu."

11. Stoga će se sadržaj temeljnih jamstava i dalje djelomično temeljiti na sudskoj praksi ESLJP-a, u mjeri u kojoj Povelja koju tumači Sud Europske unije ne predviđa višu razinu zaštite kojom se propisuju drugi zahtjevi osim sudske prakse ESLJP-a.

12. U ovom se radu objašnjavaju okolnosti i detaljnije navode četiri europska temeljna jamstva.

2. ZADIRANJA U TEMELJNA PRAVA

13. Temeljna prava na poštovanje privatnog i obiteljskog života, uključujući komunikacije, te na zaštitu osobnih podataka utvrđena su člancima 7. i 8. Povelje i primjenjuju se na sve. Nadalje, člankom 8. utvrđuju se uvjeti za zakonitost obrade osobnih podataka i priznaje pravo na pristup i ispravljanje te se nameće da ta pravila podliježu kontroli neovisnog tijela.

14. „Postupak prijenosa osobnih podataka iz države članice u treću zemlju je kao takav obrada osobnih podataka"[10]. Stoga se članci 7. i 8. Povelje primjenjuju na ovaj poseban postupak i njihova zaštita odnosi se na prenesene podatke zbog čega se ispitanicima čiji se osobni podatci prenose u treću zemlju mora osigurati razina zaštite bitno istovjetna onoj koja je zajamčena u Europskoj uniji.[11]

[8] Vidjeti t. 98. presude Schrems II.

[9] Vidjeti t. 124. spojenih predmeta C-511/18, C-512/18 i C-520/18, La Quadrature du Net i dr. (u daljnjem tekstu: La Quadrature du Net i dr.).

[10] Sud Europske unije, Schrems II, t. 83.

[11] Sud Europske unije, Schrems II, t. 96.

15. Prema mišljenju Suda Europske unije, kada se utječe na temeljno pravo na poštovanje privatnog života sadržano u članku 7. Povelje, obradom osobnih podataka pojedinca utječe se i na pravo na zaštitu podataka jer je takva obrada obuhvaćena područjem primjene članka 8. Povelje te stoga nužno mora ispuniti zahtjev za zaštitu podataka utvrđen u tom članku.[12]

16. Stoga, u pogledu mogućeg zadiranja u temeljna prava u okviru prava Unije, obveza pružatelja elektroničkih komunikacijskih usluga (…) da zadrže podatke o prometu u svrhu stavljanja tih podataka na raspolaganje, prema potrebi, nadležnim nacionalnim tijelima, postavlja pitanja koja se odnose na usklađenost s člancima 7. i 8. Povelje[13]. Isto se primjenjuje i na druge vrste obrade podataka, kao što je prijenos podataka osobama koje nisu korisnici ili pristup tim podatcima s ciljem njegove uporabe[14], što stoga podrazumijeva zadiranje u ta temeljna prava. Nadalje, pristup javnih tijela podatcima predstavlja daljnje zadiranje u skladu s ustaljenom sudskom praksom.[15]

17. Radi utvrđivanja postojanja zadiranja, nevažno je „ imaju li dotične informacije o privatnom životu osjetljiv karakter, odnosno jesu li zainteresirane osobe zbog tog zadiranja pretrpjele eventualne neugodnosti[16]". Sud Europske unije također naglašava da je moguće naknadno korištenje zadržanih podataka nevažno.[17]

18. Međutim, članci 7. i 8. Povelje nisu apsolutna prava, već se moraju uzeti u obzir u odnosu na njihovu ulogu u društvu.[18]

19. Povelja uključuje ispitivanje nužnosti i proporcionalnosti kako bi se ograničila prava koja štiti. Člankom 52. stavkom 1. Povelje određeno je područje primjene mogućih ograničenja članaka 7. i 8. navodeći da „svako ograničenje pri ostvarivanju prava i sloboda priznatih ovom Poveljom mora biti predviđeno zakonom i mora poštovati bit tih prava i sloboda. Podložno načelu proporcionalnosti, ograničenja su moguća samo ako su potrebna i ako zaista odgovaraju ciljevima od općeg interesa koje priznaje Unija ili potrebi zaštite prava i sloboda drugih osoba."

20. Sud Europske unije ponovio je da zakonodavstvo EU-a koje uključuje zadiranje u temeljna prava zajamčena člancima 7. i 8. Povelje „mora imati propisana jasna i precizna pravila kojima se uređuje doseg i primjena dotične mjere te propisivati minimalne uvjete, na način da osobe čiji se podaci prenose raspolažu dostatnim jamstvima koja omogućuju zaštitu od rizika zlouporabe", posebice ako se osobni podatci podvrgavaju automatskoj obradi i „ako postoji značajan rizik od nezakonitog pristupa tim podacima".[19]

[12] Sud Europske unije, Schrems II, t. 170. do 171.
Sud Europske unije, predmet C-623/17, Privacy International (u daljnjem tekstu:[13] Privacy International), t. 60.
[14] Sud Europske unije, Privacy International, t. 61.
[15] ESLJP, Leander, t. 48.; ESLJP, Rotaru t. 46.; Sud Europske unije, Digital Rights Ireland, t. 35.
[16] Sud Europske unije, Schrems II, t. 171., uključujući i citiranu sudsku praksu.
[17] Sud Europske unije, Schrems II, t. 171., uključujući i citiranu sudsku praksu.
[18] Sud Europske unije, Privacy International, t 63.
[19] Sud Europske unije, Privacy International, t. 68., uključujući i sudsku praksu navedenu u njemu.

21. Prema Sudu Europske unije, zaštita prava na privatnost zahtijeva da se odstupanja i ograničenja prava na zaštitu podataka „primjenjuju u mjeri u kojoj je to nužno". Nadalje, cilj od općeg interesa mora biti usklađen s temeljnim pravima na koja se mjera odnosi, „pravilnim uravnoteženjem" tog cilja u odnosu na predmetna prava.[20]

22. Slijedom toga, pristup, zadržavanje i daljnja uporaba osobnih podataka od strane javnih tijela u okviru nadzornih mjera ne smije prelaziti granice onoga što je nužno, procijenjeno u smislu Povelje, u suprotnom se „ne može smatrati opravdanim u demokratskom društvu".[21]

23. Četiri europska temeljna jamstva, kako su razrađena u sljedećem poglavlju, imaju za cilj dodatno odrediti način procjene razine zadiranja u temeljna prava na privatnost i zaštitu podataka u kontekstu nadzornih mjera javnih tijela u trećoj zemlji, pri prijenosu osobnih podataka te koje pravne zahtjeve stoga moraju primjenjivati kako bi se procijenilo bi li takva zadiranja bila prihvatljiva u skladu s Poveljom.

3. EUROPSKA TEMELJNA JAMSTVA

24. Nakon analize sudske prakse, Europski odbor za zaštitu podataka smatra da se primjenjivi pravni zahtjevi radi opravdavanja ograničenja zaštite podataka i prava privatnosti koja su priznata Poveljom mogu sažeti u četiri europska temeljna jamstva:

A. obrada bi se trebala temeljiti na jasnim, preciznim i pristupačnim pravilima,
B. nužnost i proporcionalnost u pogledu legitimnih ciljeva koji se žele postići moraju biti dokazane,
C. trebao bi postojati neovisni nadzorni mehanizam,
D. učinkoviti pravni lijekovi trebaju biti dostupni pojedincu,

25. jamstva se zasnivaju na temeljnim pravima na privatnost i zaštitu podataka koja se primjenjuju na sve, bez obzira na njihovo državljanstvo.

Jamstvo A – Obrada bi se trebala temeljiti na jasnim, preciznim i pristupačnim pravilima

26. Na temelju članka 8. stavka 2. Povelje, osobne podatke trebalo bi, među ostalim, obrađivati „u utvrđene svrhe i na temelju suglasnosti osobe o kojoj je riječ, ili na nekoj drugoj legitimnoj osnovi utvrđenoj zakonom",[22] kako je Sud Europske unije upozorio u presudi Schrems II. Nadalje, skladu s člankom 52. stavkom 1. Povelje, svako ograničenje pri ostvarivanju prava i sloboda priznatih Poveljom unutar EU-a mora biti „predviđeno zakonom". Stoga, opravdana zadiranja moraju biti u skladu sa zakonom.

[20] Sud Europske unije, Privacy International, t. 68., uključujući i sudsku praksu navedenu u njemu.
[21] Sud Europske unije, Privacy International, t. 81.
[22] Vidjeti t. 173. presude Schrems II.

27. Tom pravnom osnovom trebala bi se utvrditi jasna i precizna pravila kojima se uređuje područje primjene i primjena predmetne mjere te kojima se uvode minimalne zaštitne mjere.[23] Osim toga, Sud je upozorio da „zakonodavstvo mora biti pravno obvezujuće prema domaćem pravu"[24]. U tom je pogledu Sud razjasnio da bi se procjena mjerodavnog prava treće zemlje trebala usredotočiti na to mogu li se pojedinci pozvati na njih i istaknuti ih pred sudom.[25] Sud stoga navodi da su prava dodijeljena ispitanicima provediva. Ako pojedincima nisu dana izvršiva prava protiv javnih tijela, razina dodijeljene zaštite ne može se smatrati bitno istovjetnom onoj koja proizlazi iz Povelje, suprotno zahtjevu iz članka 45. stavka 2. točke (a) Opće uredbe.[26]

28. Nadalje, Sud je naglasio da mjerodavno pravo mora naznačiti u kojim okolnostima i pod kojim uvjetima može biti donesena mjera koja predviđa obradu takvih podataka[27] (vidjeti u nastavku pod jamstvom B za odnos između tih zahtjeva i načela nužnosti i proporcionalnosti).

29. Osim toga, Sud Europske unije također je naznačio da „svako ograničenje ostvarivanja temeljnih prava mora biti predviđeno zakonom znači da se u samoj pravnoj osnovi kojom se dopušta zadiranje u ta prava mora definirati doseg ograničenja ostvarivanja dotičnog prava".[28]

30. Konačno, Europski sud za ljudska prava „ne smatra da postoji osnova za primjenu različitih načela koja obuhvaćaju pristupačnost i jasnoću pravila kojima se uređuje presretanje pojedinih komunikacija, s jedne strane, i općenitijih programa nadzora, s druge strane."[29] ESLJP je također razjasnio da bi pravna osnova trebala uključivati barem definiciju kategorija osoba koje bi mogle podlijegati nadzoru, ograničenje trajanja mjere, postupak koji treba slijediti za pregled, korištenje i pohranu dobivenih podataka te mjere opreza koje je potrebno poduzeti pri dostavljanju podataka drugim stranama.[30]

31. Konačno, zadiranje mora biti predvidljivo u pogledu njegova učinka za pojedinca kako bi mu se pružila odgovarajuća i učinkovita zaštita od proizvoljnog zadiranja i rizika od zlouporabe. Kao rezultat toga, obrada se mora temeljiti na preciznoj, jasnoj, ali i dostupnoj (odnosno javnoj) pravnoj osnovi.[31] ESLJP je u vezi s tim pitanjem podsjetio u predmetu Zakharov da „upućivanje na ‚predvidljivost' u kontekstu presretanja komunikacija ne može biti isto kao u mnogim drugim područjima". Naveo je da u kontekstu tajnih mjera nadzora, kao što je presretanje komunikacija, „predvidljivost ne može značiti da bi pojedinac trebao moći predvidjeti kada će vlasti vjerojatno presresti njegove komunikacije kako bi mogao prilagoditi svoje ponašanje u skladu s tim". Međutim, s obzirom na to da su u takvoj situaciji očigledni rizici arbitrarnosti „nužno je imati jasna, detaljna pravila o presretanju telefonskih razgovora, posebice s obzirom na to da tehnologija dostupna za uporabu stalno postaje sofisticiranija. Domaće

[23] Vidjeti t. 175. i 180. presude Schrems II i Mišljenje 1/15 (Sporazum o PNR-u između EU-a i Kanade) od 26. srpnja 2017., t. 139. i navedenu sudsku praksu.

[24] Vidjeti t. 68. presude Privacy International – trebalo bi također biti jasno da se u francuskoj inačici presude Sud služi riječju „réglementation" koja ima šire značenje od samih akata Parlamenta.

[25] Vidjeti t. 181. presude Schrems II, u ovom se stavku Sud poziva na Predsjednički ukaz br. 28 SAD-a.

[26] Vidjeti t. 181. presude Schrems II.

[27] Vidjeti t. 68. presude Privacy International u odnosu na pravo države članice.

[28] Vidjeti presudu Schrems II, t. 175. i navedenu sudsku praksu, kao i presudu Privacy International, t. 65.

[29] ESLJP, Liberty, t. 63.

[30] ESLJP, Weber i Saravia, t. 95.

[31] ESLJP, Malone, t. 65. i 66.

pravo mora biti dovoljno jasno kako bi se građanima pružile odgovarajuće informacije o okolnostima i uvjetima pod kojima su javna tijela ovlaštena pribjeći takvim ograničenjima."[32]

Jamstvo B – Nužnost i proporcionalnost u pogledu legitimnih ciljeva koji se žele postići moraju se dokazati

32. U skladu s prvom rečenicom članka 52. stavka 1. Povelje, svako ograničenje pri ostvarivanju prava i sloboda priznatih ovom Poveljom mora biti predviđeno zakonom i mora poštovati bit tih prava i sloboda. Na temelju druge rečenice članka 52. stavka 1. Povelje, podložno načelu proporcionalnosti, ograničenja su moguća samo ako su potrebna i ako zaista odgovaraju ciljevima od općeg interesa koje priznaje Unija ili potrebi zaštite prava i sloboda drugih osoba.[33]

33. Kad je riječ o **načelu proporcionalnosti**, Sud je u odnosu na pravo države članice smatrao da pitanje potrebe opravdavanja ograničenja prava na privatnost i na zaštitu podataka mora biti procijenjeno, s jedne strane, mjerenjem **ozbiljnosti zadiranja** proizašlog takvim ograničenjem[34] i, s druge strane, provjerom da je **važnost cilja od javnog interesa** koji se nastoji ostvariti tim ograničenjem razmjerna toj ozbiljnosti.[35]

34. U predmetu La Quadrature du Net i drugi može se napomenuti da je Sud Europske unije u odnosu na pravo države članice, a ne pravo treće zemlje, odlučio da cilj zaštite nacionalne sigurnosti, zbog svoje važnosti, može opravdati mjere koje podrazumijevaju ozbiljnija zadiranja u temeljna prava za razliku od onih koje bi mogli opravdati drugi ciljevi poput borbe protiv kriminala. Međutim, utvrdio je da je to slučaj sve dok postoje dovoljno čvrsti razlozi za razmatranje suočavanja predmetne države s ozbiljnom prijetnjom nacionalnoj sigurnosti koja se pokaže istinskom i postojećom ili predvidljivom te koja podliježe ispunjenju drugih zahtjeva utvrđenih u članku 52. stavku 1. Povelje.[36]

35. U tom smislu, prema ustaljenoj sudskoj praksi Suda, odstupanja od zaštite i ograničenja zaštite osobnih podataka moraju se primjenjivati samo u mjeri u kojoj je to nužno.[37] Da bi se ispunio ovaj uvjet, propis mora imati propisana jasna i precizna pravila kojima se uređuju doseg i primjena dotične mjere te nalagati minimalne uvjete, tako da osobe čiji su podatci preneseni raspolažu dostatnim jamstvima

[32] ESLJP, Zakharov, t. 229.

[33] Schrems II, t. 174.

[34] U tom je kontekstu Sud, primjerice, napomenuo da se „zadiranje, koje podrazumijeva prikupljanje podataka u stvarnom vremenu koji omogućuju određivanje lokacije terminalne opreme, proizlazi da je osobito ozbiljno jer se tim podacima daje nacionalnim nadležnim tijelima precizno i trajno sredstvo za praćenje kretanja korisnika prijenosnih telefona. (...)" (La Quadrature du Net i dr., t. 187., uključujući navedenu sudsku praksu).

[35] La Quadrature du Net i dr., t. 131.

[36] Točke 136. i 137. Vidjeti i presudu Privacy International, s obzirom na to da je Sud odredio da se takve prijetnje zbog svoje prirode i posebne ozbiljnosti razlikuju po svojoj naravi i posebnoj težini od općeg rizika nastanka napetosti ili poremećaja koji će utjecati na javnu sigurnost. Točka 75. Primjerice, u predmetu La Quadrature du Net i dr., Sud je napomenuo da automatizirana analiza podataka o prometu i lokaciji koja općenito i bez diskriminacije obuhvaća podatke osoba koje upotrebljavaju elektroničke komunikacijske sustave predstavlja posebno ozbiljno zadiranje tako da takva mjera može ispuniti zahtjev proporcionalnosti samo u situacijama u kojima se predmetna država članica suočava s ozbiljnom prijetnjom nacionalnoj sigurnosti koja se pokaže istinskom i prisutnom ili predvidljivom te, među ostalim uvjetima, pod uvjetom da je trajanje zadržavanja ograničeno na ono što je nužno (t. 174. do 177.).

[37] Schrems II, t. 176., uključujući i citiranu sudsku praksu.

koja omogućuju djelotvornu zaštitu njihovih osobnih podataka od rizika zlouporabe. „On mora osobito navesti u kojim se okolnostima i pod kojim uvjetima može donijeti mjera kojom se predviđa obrada takvih podataka, na taj način osiguravajući da zadiranje bude ograničeno na ono što je strogo nužno. Nužnost posjedovanja takvih jamstava još je značajnija kad su osobni podaci podvrgnuti automatskoj obradi."[38]

36. U presudi Schrems II, Sud Europske unije naglasio je da zakonodavstvo treće zemlje u kojem nisu propisana ograničenja u njemu sadržanih ovlasti za provođenje programa nadzora radi prikupljanja stranih obavještajnih informacija ne može osigurati razinu zaštite koja je bitno istovjetna onoj zajamčenoj Poveljom. Zaista, u skladu sa sudskom praksom, pravna osnova kojom se dopušta zadiranje u temeljna prava mora, u skladu s načelom proporcionalnosti, definirati doseg ograničenja ostvarivanja dotičnog prava.[39]

37. U pogledu **načela nužnosti**, Sud Europske unije jasno je pokazao kako zakonodavstva kojima se „dopušta pohranjivanje svih osobnih podataka svih osoba čiji su podaci preneseni iz Europske unije (...) bez ikakvog razlikovanja, ograničenja ili iznimke s obzirom na postavljeni 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, strogo ograničene i mogu opravdati zadiranje koje obuhvaća i pristup i uporabu tih podataka " ne ispunjavaju to načelo[40]. Posebice se zakoni kojima se javnim tijelima omogućava općenit pristup sadržaju elektroničkih komunikacija moraju smatrati povredom bîti temeljnog prava na poštovanje privatnog života koje je zajamčeno u članku 7. Povelje.[41]

38. Isto tako, ali ovaj put tijekom procjene prava države članice, a ne prava treće zemlje, Sud Europske unije utvrdio je u predmetu La Quadrature du Net i dr. da „zakonodavstvo koje zahtijeva zadržavanje osobnih podataka mora uvijek ispunjavati objektivne kriterije kojima se uspostavlja veza između zadržanih podataka i cilja koji se želi postići."[42] U istom kontekstu, u presudi Privacy International, također je zaključio da zakonodavac, odnosno propis „mora se temeljiti na objektivnim kriterijima kako

[38] Schrems II, t. 175.

[39] Schrems II, t. 180.

[40] Schrems I, t. 93. s daljnjim upućivanjima. Međutim, ovaj put u odnosu na pravo države članice, a ne pravo treće zemlje, vidjeti presudu Privacy International, t. 71., uključujući navedenu sudsku praksu. U tom je slučaju Sud naveo da nacionalni propis koji pružateljima elektroničkih komunikacijskih usluga nalaže da sigurnosnim i obavještajnim službama općenito i neselektivno prijenosom otkrivaju podatke o prometu i lokaciji, prekoračuje granice onog što je strogo nužno i ne može se smatrati opravdanim u demokratskom društvu, kako nalaže Direktiva o privatnosti i elektroničkoj komunikaciji, tumačeno s obzirom na Povelju (članak 81.).

[41] Schrems I, t. 94.

[42] La Quadrature du Net i dr., t. 133. U tom kontekstu, Sud je potvrdio da su zakonodavne mjere koje kao preventivnu mjeru omogućavaju opće i neselektivno zadržavanje podataka o prometu i lokaciji isključene Direktivom o privatnosti i elektroničkoj komunikaciji, tumačeno s obzirom na Povelju. Suprotno tomu, Sud je presudio da u situacijama ozbiljne ugroze nacionalne sigurnosti koja se pokaže istinskom i postojećom ili predvidljivom, zakonodavac može dopustiti, radi zaštite nacionalne sigurnosti, korištenje uputom kojom se od pružatelja elektroničkih komunikacijskih usluga zahtijeva da zadrže, općenito i bez diskriminacije, podatke o prometu i lokaciji. Međutim, takva mjera mora ispuniti posebne uvjete. Točnije, uputa se može dati samo u vremenskom razdoblju koje je ograničeno na ono što je nužno, a koje se može produljiti ako ta prijetnja ustraje (t. 168.).

bi definirao okolnosti i uvjete u kojima nadležnim nacionalnim tijelima treba biti odobren pristup predmetnim podacima".[43]

Jamstvo C – Neovisan nadzorni sustav

39. Europski odbor za zaštitu podataka podsjeća da je došlo do zadiranja u vrijeme prikupljanja podataka, ali i u trenutku pristupa podatcima tijela javne vlasti u svrhu daljnje obrade. ESLJP je više puta precizirao da svako zadiranje u pravo na privatnost i zaštitu podataka treba podlijegati učinkovitom, neovisnom i nepristranom sustavu nadzora koji mora osigurati sudac ili drugo neovisno tijelo[44] (primjerice, upravno tijelo ili parlamentarno tijelo). U presudi Schrems II, Sud EU-a također je uzeo u obzir neovisni nadzor nad provedbom mjera nadzora.[45]

40. ESLJP navodi da se, iako je prethodno (pravosudno) odobrenje nadzornih mjera važna zaštita od arbitrarnosti, mora uzeti u obzir i stvarno funkcioniranje sustava presretanja, uključujući provjere i ravnoteže u izvršavanju ovlasti te postojanje ili odsustvo stvarne zloporabe.[46] U predmetu Schrems II, Sud Europske unije uzeo je u obzir i opseg nadzorne uloge mehanizma nadzora kojim nisu obuhvaćene pojedinačne mjere nadzora.[47]

41. U pogledu prava država članica, Sud Europske unije utvrdio je niz mjera koje su u skladu s pravom Unije samo ako podliježu učinkovitom preispitivanju koje provodi sud ili neovisno upravno tijelo čija je odluka obvezujuća. Cilj je tog preispitivanja provjeriti postoji li situacija koja opravdava mjeru i poštuju li se uvjeti i zaštitne mjere koji se moraju utvrditi[48]. Za prikupljanje podataka o prometu i lokaciji u stvarnom vremenu, preispitivanjem bi se trebalo omogućiti da se *ex ante* provjerom utvrdi, među ostalim, je li ono dopušteno samo u granicama onoga što je nužno. U opravdanim hitnim situacijama mjere mogu biti provedene bez takvog prethodnog preispitivanja. Međutim, Sud i dalje zahtijeva da se naknadno preispitivanje provede u kratkom roku.[49]

42. U pogledu neovisnosti nadzornih mehanizama u vezi s nadzorom, mogli bi se uzeti u obzir zaključci Suda Europske unije o neovisnosti tijela u kontekstu pravne zaštite (vidjeti u nastavku pod jamstvom D). Nadalje, sudska praksa ESLJP-a može ponuditi dodatne elemente. Sud je izrazio želju da sudac bude odgovoran za održavanje nadzora. Međutim, nije isključeno da drugo tijelo može biti odgovorno „sve dok je dovoljno neovisno od izvršnog tijela"[50] i „tijela koja provode nadzor i ima dovoljno ovlasti i nadležnosti za provedbu djelotvorne i kontinuirane kontrole". [51]ESLJP je dodao da tijekom procjene

[43] Privacy International, t. 78., uključujući navedenu sudsku praksu. U presudi Privacy International, u pogledu pristupa nadležnog tijela osobnim podatcima u okviru prava države članice, Sud je odlučio da se „opći pristup svim zadržanim podacima, neovisno o tome postoji li ikakva veza, bilo i posredna, s ciljem koji se nastoji postići, ne može smatrati ograničenim na ono što je strogo nužno, (t. 77. do 78.).

[44] ESLJP, Klass, t. 17., 51.

[45] Schrems II, t. 179., 183.

[46] ESLJP, predmet Big Brother Watch, pobijana presuda, t. 319. do 320.

[47] Schrems II, t. 179.

[48] Sud Europske unije, La Quadrature du Net i dr., t. 168., 189.

[49] Sud Europske unije, La Quadrature du Net i dr., t. 189.

[50] ESLJP, Zakharov, t. 258., Iordachi i dr. protiv Moldavije, t. 40. i 51., i Dumitru Popescu protiv Rumunjske, t. 70. do 73.

[51] ESLJP, Klass, t. 56. i Big Brother Watch, pobijana presuda, t. 318.

neovisnosti[52] treba uzeti u obzir „način imenovanja i pravni status članova nadzornog tijela". To uključuje „osobe kvalificirane za obnašanje pravosudnih dužnosti koje imenuje parlament ili premijer. Nasuprot tome, utvrđeno je da ministar unutarnjih poslova nije samo bio politički kandidat i član izvršne vlasti, već je izravno sudjelovao u puštanju u rad posebnih načina nadzora, nije dovoljno neovisan."[53] ESLJP također „primjećuje da je od ključne važnosti da nadzorno tijelo ima pristup svim predmetnim dokumentima, uključujući zatvorene materijale"[54]. Konačno, ESLJP uzima u obzir „jesu li aktivnosti nadzornog tijela otvorene za javni nadzor".[55]

Jamstvo D – Učinkoviti pravni lijekovi trebaju biti dostupni pojedincu

43. Posljednje europsko temeljno jamstvo povezano je s pravima pojedinca na pravnu zaštitu. On/a mora imati učinkovit pravni lijek kako bi ispunio/la svoja prava kada on/a smatra da se ta prava ne poštuju ili da nisu bila poštovana. Sud Europske unije opisao je u presudi Schrems I da „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. Prvi stavak članka 47. Povelje obvezuje da svatko čija su prava i slobode zajamčeni pravom Unije povrijeđeni ima pravo na djelotvoran pravni lijek pred sudom, u skladu s uvjetima utvrđenima ovim člankom."[56]

44. Tijekom procjene prava države članice kojima se omogućuje prikupljanje podataka o prometu i lokaciji u stvarnom vremenu, Sud je smatrao da je slanje obavijesti potrebno „da se tim osobama omogući da se koriste svojim pravima koja proizlaze iz članaka 7. i 8. Povelje, da zahtijevaju pristup svojim osobnim podacima koji su predmet tih mjera te, po potrebi, njihov ispravak ili brisanje, kao i da, u skladu s člankom 47. prvim stavkom Povelje, podnesu djelotvoran pravni lijek pred sudom".[57] Međutim, također je priznao da se obavješćivanje osoba čiji su podaci prikupljeni ili analizirani mora obaviti samo u onoj mjeri u kojoj su ta tijela odgovorna i do trenutka kada ta obavijest prestane ugrožavati zadatke za koje su ta tijela odgovorna.[58]

45. I za ESLJP je pitanje učinkovitog pravnog lijeka neodvojivo povezano i sa slanjem obavijesti mjere nadzora pojedincu nakon završetka nadzora. Sud je posebno utvrdio da „u načelu nema dovoljno prostora da dotični pojedinac pribjegne sudovima osim ako se tom pojedincu ne savjetuje o mjerama poduzetima bez njegova znanja i ako on samim tim može retrospektivno osporiti njihovu zakonitost ili, alternativno, osim ako svaka osoba koja sumnja da su njegove komunikacije presretnute ili su bile presretnute ima pravo na djelotvoran pravni lijek, tako da nadležnost sudova ne ovisi o obavijesti subjektu presretanja da je došlo do presretanja njegovih komunikacija."[59] Stoga je ESLJP priznao da u nekim slučajevima možda neće postojati obavijest, ali da se mora osigurati učinkovit pravni lijek. U tom je slučaju Sud Europske unije, primjerice u predmetu Kennedy, jasno utvrdio da sud nudi dostatne mogućnosti pravne zaštite, ako ispunjava niz kriterija, odnosno ako ima neovisno i nepristrano tijelo

[52] ESLJP, Zakharov, t. 278.
[53] ESLJP, Zakharov, t. 278.
[54] ESLJP, Zakharov, t. 281.
[55] ESLJP, Zakharov, t. 283.
[56] Sud Europske unije, Schrems I, t. 95.
[57] Vidjeti t. 190. presude La Quadrature du Net i dr., i mišljenje Suda Europske unije 1/15, t.k 220.
[58] Vidjeti t. 191. presude La Quadrature du Net i dr.
[59] ESLJP, Zakharov, t. 234.

koje je donijelo vlastiti poslovnik, koje je sastavljeno od članova koji moraju obnašati ili imati visoke sudske dužnosti ili imati iskusne pravnike te da ne postoji očit teret koji treba prevladati kako bi mu se podnio zahtjev.[60] Tijekom ispitivanja pritužbi pojedinaca, sud bi trebao imati pristup svim relevantnim informacijama,[61] uključujući zatvorene materijale. Konačno, sud bi trebao imati ovlasti za ispravljanje neusklađenosti.[62]

46. Članak 47. Povelje upućuje na sud (*eng. tribunal*), iako se u jezičnim inačicama koje nisu engleske preferira riječ „sud" (*eng. court*),[63] a ESLJP samo obvezuje države članice da osiguraju da „svi koji krše svoja prava i slobode imaju učinkovit pravni lijek pred nacionalnim tijelom"[64] koji ne mora nužno biti pravosudno tijelo.[65]

47. Sud Europske unije ponavlja, u kontekstu presude Schrems II, tijekom ocjenjivanja prikladnosti razine zaštite treće zemlje „da pojedinci moraju imati mogućnost korištenja pravnim sredstvima pred neovisnim i nepristranim sudom radi pristupa osobnim podacima koji se na njih odnose ili ispravka ili brisanja takvih podataka."[66] U tom istom kontekstu, Sud Europske unije smatra da učinkovita pravna zaštita od takvih zadiranja ne može biti zajamčena samo sudom, već i tijelom[67] koje nudi jamstva koja su bitno ekvivalentna onima obveznim na temelju članka 47. Povelje. U svojoj presudi Schrems II, Sud Europske unije istaknuo je da se neovisnost suda ili tijela mora osigurati, posebno od izvršnog tijela, svim potrebnim jamstvima, uključujući u pogledu njegovih uvjeta za razrješenje s dužnosti ili opoziv imenovanja,[68] te da ovlasti koje bi trebalo dodijeliti sudu moraju biti u skladu sa zahtjevima iz članka 47. Povelje. U tom pogledu, tijelu[69] se daje ovlast za donošenje odluka koje su obvezujuće za obavještajne službe, u skladu s pravnim zaštitnim mjerama na koje se subjekti obrade podataka mogu osloniti.[70]

4. ZAVRŠNE NAPOMENE

48. Četiri europska temeljna jamstva smatraju se ključnim elementima koji se mogu pronaći tijekom ocjenjivanja razine zadiranja u temeljna prava na privatnost i zaštitu podataka. Ne bi ih trebalo ocjenjivati neovisno jer su usko povezana, već općenito, preispitivanjem relevantnog zakonodavstva u pogledu nadzornih mjera, minimalne razine zaštitnih mjera za zaštitu prava ispitanika i pravnih lijekova predviđenih nacionalnim pravom treće zemlje.

---

[60] ESLJP, Kennedy, t. 190.

[61] Europski odbor za zaštitu podataka napominje da povjerenik Vijeća Europe za ljudska prava smatra da se takozvano pravilo „trećih strana" – na temelju kojeg obavještajne službe u jednoj državi koja pruža podatke obavještajnim agencijama u drugim državama mogu agencijama primateljima nametnuti obvezu da ne otkrivaju prenesene podatke nijednoj trećoj strani – ne bi trebalo primjenjivati na nadzorna tijela kako se ne bi narušila mogućnost djelotvornog pravnog lijeka (Publikacija o demokratskom i učinkovitom nadzoru nacionalnih sigurnosnih službi).

[62] ESLJP, Kennedy, t. 167.

[63] Riječ sud (*eng. tribunal*) je, primjerice, prevedena kao „Gericht" na njemačkom i „gerecht" na nizozemskom.

[64] Članak 13. EKLJP-a.

[65] ESLJP, Klass, t. 67.

[66] Vidjeti t. 194. presude Schrems II.

[67] Vidjeti t. 197. presude Schrems II u kojoj Sud izričito upotrebljava ovu riječ.

[68] Vidjeti t. 195. presude Schrems II.

[69] Vidjeti t. 197. presude Schrems II u kojoj Sud izričito upotrebljava ovu riječ.

[70] Vidjeti t. 196. presude Schrems II.

49. Ta jamstva zahtijevaju određeni stupanj tumačenja, posebice s obzirom na to da zakonodavstvo treće zemlje ne mora biti istovjetno pravnom okviru EU-a.

50. Kao što je ESLJP naveo u predmetu Kennedy, „procjena ovisi o svim okolnostima predmeta, kao što su priroda, opseg i trajanje mogućih mjera, razlozi potrebni za njihovo naređivanje, tijela nadležna za njihovo odobravanje, provedbu i nadzor te vrsta pravnog lijeka predviđena nacionalnim pravom”.[71]

51. Stoga procjena mjera nadzora treće zemlje u odnosu na europska temeljna jamstva može dovesti do dva zaključka:

- Predmetnim zakonodavstvom treće zemlje ne osiguravaju se zahtjevi iz europskih temeljnih jamstava: u ovom slučaju zakonodavstvo treće zemlje ne bi pružilo razinu zaštite koja je bitno istovjetna onoj zajamčenoj u EU-u.

- Predmetno zakonodavstvo treće zemlje zadovoljava europska temeljna jamstva.

52. Tijekom procjene prikladnosti razine zaštite, Komisija će u skladu s člankom 45. Opće uredbe morati ocijeniti jesu li europska temeljna jamstva zadovoljena kao dio elemenata za koje će se smatrati da jamče da zakonodavstvo treće zemlje u cjelini nudi razinu zaštite koja je bitno istovjetna onoj zajamčenoj u EU-u.

53. Kada se izvoznici podataka, zajedno s uvoznicima podataka, oslanjaju na odgovarajuće zaštitne mjere u skladu s člankom 46. Opće uredbe, s obzirom na zahtjeve zakonodavstva treće zemlje koje se posebno primjenjuje na prenesene podatke, trebali bi osigurati učinkovito ostvarivanje bitno istovjetne razine zaštite. Točnije, ako pravo treće zemlje nije u skladu sa zahtjevima iz europskih temeljnih jamstava, to bi značilo da se predmetnim zakonom neće utjecati na jamstva i zaštitne mjere koji se odnose na prijenos kako bi se i dalje pružala razina zaštite koja je bitno istovjetna onoj zajamčenoj u EU-u.

54. Europski odbor za zaštitu podataka izdao je dodatne smjernice i preporuke koje treba uzeti u obzir za nastavak procjene, ovisno o alatu za prijenos koji će se koristiti i o potrebi za pružanjem odgovarajućih zaštitnih mjera, uključujući, ovisno o slučaju, dodatne mjere.[72]

55. Nadalje, valja napomenuti da se europska temeljna jamstva temelje na onome što je propisano zakonom. Europski odbor za zaštitu podataka naglašava da se europska temeljna jamstva zasnivaju na temeljnim pravima koja se primjenjuju na sve, bez obzira na njihovo državljanstvo.

56. Europski odbor za zaštitu podataka ponavlja da su europska temeljna jamstva referentne norme tijekom procjene zadiranja koja proizlaze iz mjera nadzora trećih zemalja u kontekstu međunarodnih prijenosa podataka. Te norme proizlaze iz prava Unije i sudske prakse Suda Europske unije i Europskog suda za ljudska prava, koji su obvezujući za države članice.

[71] ESLJP, Kennedy, t. 153.

Adequacy Referential, WP 254 rev. 01., revidiran i donesen 16. veljače 2018.; Preporuke Europskog odbora za zaštitu podataka 01/2020 o mjerama kojima se dopunjuju alati za prijenos kako bi se osigurala usklađenost s razinom zaštite osobnih podataka EU-a, 10. studenoga 2020.[72]