OBVEZNO ZADRŽAVANJE PODATAKA I PRIVATNOST

Prof. dr. sc. Dražen Dragičević [*]
Dr. sc. Nina Gumzej [**]

UDK: 342.738(4)EU
35.083.8(4)EU
339,923:061.1>(4)EU
Izvorni znanstveni rad
Primljeno: siječanj 2013.

Autori u radu analiziraju pravno uređenje sustava obveznog preventivnog zadržavanja podataka koji se generiraju, odnosno obrađuju u vezi s pružanjem javno dostupnih elektroničkih komunikacijskih usluga ili javnih komunikacijskih mreža u pravu EU-a i RH.

Brojna otvorena pitanja u vezi s uvođenjem i provedbom tog sustava ispituju se s obzirom na osjetljivost i poseban tretman koji podaci u elektroničkim komunikacijama imaju u pravu EU-a općenito, a osobito s obzirom na veliku mogućnost zadiranja u temeljna prava i slobode korisnika usluga – građana, posebno kada je riječ o poštovanju privatnog života i tajnosti dopisivanja, tj. komunikacije, te pravu na zaštitu osobnih podataka.

U radu se analiziraju i najnoviji događaji u vezi s provedbom Direktive o zadržavanju podataka u EU-u, njezinom ocjenom te postupcima pokrenutim pred Sudom pravde Europske unije. Autori također ispituju i analiziraju rješenja koja su, radi usklađivanja našeg zakonodavstva s acquisom, *tj. Direktivom o zadržavanju podataka, predviđena u domaćem pravnom okviru, kao i ona koja su otprije na snazi (neovisno o Direktivi) te iznose prijedloge rješenja* de lege ferenda *gdje to nalaze potrebnim.*

Prilikom uređenja ovlaštenja za pristup relevantnim podacima, među ostalim, upozorava se i na nužnost dosljedne provedbe kriterija za iznimno ograničavanje zajamčenih prava građana u opravdanim, jasno utvrđenim slučajevima te na

[*] Dr. sc. Dražen Dragičević, profesor Pravnog fakulteta Sveučilišta u Zagrebu, Trg maršala Tita 14, Zagreb

[**] Dr. sc. Nina Gumzej, viša asistentica Pravnog fakulteta Sveučilišta u Zagrebu, Trg maršala Tita 14, Zagreb

nužnost osiguravanja što preciznijih i jasnijih zakonodavnih rješenja radi sprečavanja mogućih zloporaba.

Ključne riječi: Direktiva o zadržavanju podataka, prometni podaci, tajnost komunikacija, privatnost, zaštita osobnih podataka

1. UVOD

Zahtjevi nadležnih tijela da se uvede obveza prikupljanja i pohrane podataka o elektroničkim komunikacijama[1] radi učinkovitije borbe protiv kriminala i zaštite nacionalne sigurnosti osobito su postali izraženi nakon terorističkih napada u SAD-u i Europi početkom prošlog desetljeća.[2] Uskoro nakon toga u pojedinim državama Europske unije uslijedile su zakonodavne aktivnosti usmjerene na propisivanje mjera obveznog zadržavanja podataka u elektroničkim komunikacijama. Potreba usklađivanja takvih mjera na razini prava Europske unije dovela je do usvajanja *Direktive 2006/24/EZ o zadržavanju podataka generiranih ili obrađenih u vezi s pružanjem javno dostupnih elektroničkih komunikacijskih usluga ili javnih komunikacijskih mreža* (dalje u tekstu: Direktiva o zadržavanju podataka ili Direktiva).[3] Međutim, još od prvih prijedloga četiriju država članica EU-a da se mjera uredi (Okvirnom odlukom Vijeća EU-a), što je Europski parlament odbio[4], postavljala su se pitanja oko njezine *nužnosti* i

[1] Predlagatelji su to argumentirali okolnošću da nedostupnost prometnih podataka za potrebe tijela progona dolazi sve više do izražaja zbog razvoja novih poslovnih modela, a osobito besplatnih elektroničkih komunikacijskih usluga i usluga čiji obračun ne ovisi o korištenom prometu (npr. *flat-rate*, *prepaid* tarife) i koje operatori, prema tome, ne zadržavaju u tu svrhu. *Proposal for a Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC*, COM(2005) 438 final - 2005/0182 (COD), 21. rujna 2005., str. 2.

[2] Vidi Deklaraciju Europskog vijeća o suzbijanju terorizma: Declaration on combating terrorism, 25. ožujka 2004., http://www.consilium.europa.eu/ uedocs/cmsUpload/DECL-25.3.pdf (30. prosinca 2013.).

[3] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications network, OJ L 105, 13. travnja 2006., str. 54 – 63.

[4] European Parliament, *Report on the initiative by the French Republic, Ireland, the Kingdom of Sweden and the United Kingdom for a Draft Framework Decision on retention of data processed and stored in connection with the provision of publicly available electronic communications services or data on public communications networks for the purpose of prevention, investigation, detection and prosecution of crime and criminal offences including terrorism (8958/2004-C6 0198/2004-2004/0813(CNS)*, final A6-0174/2005, 31. svibnja 2005.

osobito *razmjernosti s obzirom na cilj koji se njome treba postići*. Naime, zadržavanje velike količine osjetljivih podataka koji se odnose na komuniciranje svih korisnika usluga, bez obzira na postojanje ikakve sumnje na počinjenje kaznenog djela, a radi eventualne potrebe za pojedinim podacima malog broja njih u budućnosti, uz sve brojnije i naprednije mogućnosti analiza i profiliranja, mjera je kojom se izrazito intenzivno zadire u njihova temeljna prava i slobode. Posebno se smatralo da se ovime znatno ograničava temeljno pravo privatnosti u vidu prava na poštovanje privatnog života i tajnost dopisivanja, kako se ono jamči člankom 8. *Europske konvencije za zaštitu ljudskih prava i temeljnih sloboda* (dalje u tekstu: Europska konvencija).[5] S obzirom na opisana svojstva mjere zadržavanja smatralo se da njezinu uređenju na razini prava EU-a mora prethoditi nesporno dokazana nužnost s obzirom na zaštićeni pravni interes i da treba voditi više računa o razmjernosti mjere. S time u vidu postavljalo se i pitanje potrebe ulaganja većih napora radi učinkovitije provedbe mjere hitne zaštite pohranjenih računalnih podataka, koja se temelji na *Konvenciji Vijeća Europe o kibernetičkom kriminalu*.[6] No ovo nije imalo ozbiljnijeg odjeka jer je mjera zadržavanja ubrzo propisana u formi direktive u prvom stupu Zajednice, tj. na temelju odredbi o funkcioniranju unutarnjeg tržišta, a ranije navedena sporna pitanja dotaknuta su afirmacijama u vezi s nužnošću uvođenja mjere zadržavanja i osiguranih jamstava prava na poštovanje privatnog života i tajnosti komunikacija te prava na zaštitu osobnih podataka.[7] Svrha zadržavanja prema Direktivi osiguravanje je dostupnosti podataka radi *istrage, otkrivanja i progona teških kaznenih djela* kako ih svaka država članica EU-a definira u domaćem pravu. Države članice tako su postale dužne osigurati zadržavanje u unutarnjem pravu s temeljnom obvezom davatelja javno dostupnih elektroničkih komunikacijskih usluga i javnih komunikacijskih mreža na pohranjivanje podataka u elektroničkim komunikacijama svih njihovih korisnika, uključivo identifikacijskih podataka, u roku koji nije smio biti kraći od šest mjeseci i u pravilu ne dulji od dvije godine. Pokušaj poništenja Direktive pred Sudom pravde Europske unije (dalje u tekstu: Europski sud) uslijedio je već 2006. g. Ta se tužba zasnivala na argumentu da je mjera trebala biti usvojena jednoglasno (jednoglasja u Vijeću EU-a nije bilo) u trećem stupu Zajednice, tj. prema odredbama o policijskoj i pravosudnoj suradnji u kaznenim predmetima. Europski sud tužbu je odbio, smatrajući da je mjera pravilno donesena u prvome

[5] Convention for the protection of human rights and fundamental freedoms (CETS No. 005), 4. studenoga 1950.

[6] Council of Europe, *Convention on Cybercrime* (CETS No. 185), 23. studenoga 2001.

[7] Recitali 9. i 22. Direktive o zadržavanju podataka.

stupu i to s ciljem osiguravanja da se ujednačenim pravilima spriječi daljnji utjecaj različitih rješenja obveznog zadržavanja unutar EU-a na unutarnje tržište (osobito u pogledu vrsti podataka, rokova, zaštitnih mjera), što su velika opterećenja i troškovi za operatore. Za ovaj rad bitno je istaknuti tumačenje Suda da se Direktiva odnosi na obveze i aktivnosti operatora, a ne na aktivnosti tijela za provedbu zakona kao što su npr. pristup zadržanim podacima i njihovo korištenje.[8]

Danas, sedam godina nakon donošenja Direktive i nakon prvog izvješća Europske komisije o njezinoj provedbi i ocjeni, situacija u državama članicama takva je da je u većini njih Direktiva transponirana, ali neujednačeno. Usklađivanje koje se Direktivom trebalo osigurati nije postignuto, a osim toga u pojedinim su državama relevantne odredbe unutarnjeg prava u vezi s time i ukidane pretežito u ustavnosudskim postupcima. Čini se intenzivnije nego ikada do sada, a nastavno na raspoložive podatke o provedbi Direktive, vrlo ozbiljno se i na razini relevantnih institucija EU-a pristupa preispitivanju razmjernosti i nužnosti zadržavanja prema Direktivi te potrebi utvrđivanja učinkovitijih zaštitnih mehanizama, a svakako osiguravanju jače harmonizacije u EU-u. Osim toga, situacija u pravu EU-a uvelike se promijenila od donošenja Direktive, a to uključuje i izmjene u raspodjeli nadležnosti EU-a i država članica s utjecajem na ovo područje i novu opću pravnu osnovu za uređenje zaštite osobnih podataka koje je dobilo status zasebnog temeljnog prava. Zbog intenzivnog ograničavanja prava i sloboda, poglavito (ali ne isključivo[9]) prava na privatnost i zaštitu osobnih podataka, kritičari Direktive sve glasnije traže ozbiljnija istraživanja o mogućim alternativnim mjerama, poput ranije spomenute hitne zaštite podataka i/ili sličnog. Osim toga, osviještenost javnosti u EU-u evidentno je porasla zadnjih godina, a u skladu s time i kritičnije razmatranje rješenja zadržavanja kako prema pravu EU-a tako i prema domaćem pravu te u skladu s Europskom konvencijom, što je u pojedinim državama dovelo i do ukidanja relevantnih odredbi i/ili propisa najčešće u ustavnosudskim

[8] Vidi C-301/06 *Ireland v European Parliament and Council*, (2009) ECR, I-00593, usporedi s proceduralnim razlozima za odbijanje inicijalnog prijedloga uređenja Okvirnom odlukom, *supra* bilj. 4, te s ranijom odlukom Europskog suda kojom je poništen sporazum između EU-a i SAD-a o obradi i prijenosu podataka o putnicima u SAD u svrhu borbe protiv terorizma i drugih teških kaznenih djela poput organiziranog kriminala: C-317/04 i 318/04 *European Parliament v Council (C-317/04) and Commission (C-318/04)*, (2006) ECR, I-04721.

[9] U radu nećemo analizirati utjecaj na druga prava i slobode, kao npr. slobodu izražavanja, na koju također utječe mjera obveznog preventivnog zadržavanja podataka u elektroničkim komunikacijama.

postupcima. Svemu tome treba pridodati činjenicu da su do danas pokrenuta već dva prethodna postupka pred Europskim sudom sa zahtjevima za ocjenu sukladnosti Direktive s jamstvima temeljnih prava i sloboda (u većem broju slučajeva domaći sudovi nisu prihvaćali prijedloge da se po tim pitanjima pokrene prethodni postupak).

Republika Hrvatska je već 2008. g. implementirala Direktivu, a osim toga obvezno zadržavanje podataka u elektroničkim komunikacijama u domaćem je pravnom okviru na snazi i od ranije (neovisno o Direktivi). Iako je riječ o važnoj temi koja se, osobito unutar EU-a, sve ozbiljnije razmatra ne samo u pogledu zaštite prava i sloboda, već i zbog niza drugih razloga s obzirom na sve uključene interese (unutarnja sigurnost, kaznenopravna zaštita, neometani rad unutarnjeg tržišta EU-a i dr.), zamijetili smo da ona u domaćoj literaturi nije značajnije obrađena s težištem na ispitivanju aspekta zaštite ljudskih prava, poglavito prava na privatnost i zaštitu osobnih podataka. Cilj je našeg rada pretežito gledano iz potonjeg aspekta dati doprinos razvoju daljnjeg znanstvenog istraživanja teme u Republici Hrvatskoj i to kroz komparativnu pravnu analizu te ispitivanje razvojnih momenata i aktualnosti oko uređenja sustava zadržavanja podataka prema pravu EU-a i domaćem pravu, a u skladu s jamstvima ograničenja navedenih temeljnih prava.

2. PRAVNI OKVIR

2.1. Privatnost i zaštita osobnih podataka – temeljna prava

Kod razmatranja temeljnih prava i sloboda u koja se zadire opisanom mjerom preventivnog zadržavanja podataka u ovome radu usredotočujemo se na pravo na privatnost, uzimajući osobito u obzir jamstva poštovanja prava na privatni život i tajnost dopisivanja prema članku 8. Europske konvencije. Ta se zaštita svakako proteže na sam sadržaj komunikacije (podatke koji su sadržaj komunikacije), neovisno o tome odvijala se ona putem telefona, telefaksa, e-pošte, *pagera* ili pregledavanjem interneta.[10] U ovome pogledu zaštitu pred

[10] Vidi npr. *Kvasnica v Slovakia* (zahtjev br. 72094/01), 9. lipnja 2009., stavak 76; *Liberty and others v The United Kingdom* (zahtjev br. 58243/00), 1. srpnja 2008., ECHR 2008, stavak 56; *Gabriele Weber and Cesar Richard Saravia v Germany* (zahtjev br. 54934/00), 29. lipnja 2006., ECHR 2006-XI, stavak 77; *Taylor-Sabori v The United Kingdom* (zahtjev br. 47114/99), 22. listopada 2002., stavci 16 – 19; *Malone v the United Kingdom* (zahtjev br. 8691/79), 2. kolovoza 1984., Serija A, br. 82, stavak 64; *Halford v the United Kingdom*, 25. lipnja 1997., Reports 1997-III, stavci 42 – 46 i 52; *Copland v The United Kingdom* (zahtjev br. 62617/00), 3. travnja 2007., ECHR 2007-I, stavci 41 – 44. Vidi i *P. G. and J. H. v The United Kingdom* (zahtjev

Europskim sudom za ljudska prava (dalje u tekstu i: Sud) često su tražile osobe nad kojima su se provodile mjere tajnog nadzora komunikacija. Telefonski razgovori prema praksi Suda obuhvaćeni su pojmom privatnog života i pojmom dopisivanja (komunikacije) u smislu članka 8. Europske konvencije i s ovime u vidu mjera tajnog nadzora razgovora već je sama po sebi zadiranje u izvršavanje prava pojedinca.[11] Osim u pogledu mjera tajnog nadzora komunikacija, Sud je u svojoj praksi štitio pravo na privatni život i tajnost dopisivanja i u vezi s mjerama za koje je utvrdio da podrazumijevaju manju razinu zadiranja u ta prava. Tako je Sud npr. kod mjera nadzora koje su se sastojale od pristupa i čuvanja, tj. obrade prometnih podataka (podaci o pozivanim brojevima, vremenu i duljini trajanja razgovora) ocijenio da se ti podaci mogu smatrati dijelom komunikacije osoba.[12] Zaštita prava na privatni život i tajnost dopisivanja proteže se i na podatke u vezi s korištenjem interneta i e-pošte.[13] Iako Europska konvencija izričito ne jamči pravo na zaštitu osobnih podataka, u praksi Suda ovo pravo smatra se od temeljne važnosti za uživanje prava na privatni život (čl. 8.) pa tako npr. zadiranje u to pravo predstavlja bilježenje i pohranjivanje (u tajnom policijskom registru) podataka koji se odnose na privatni život osobe[14], a povreda može nastupiti i ako država ne ispunjava pozitivne obveze radi osiguravanja uvjeta za poštovanje prava pojedinca.[15]

---

br. 44787/98), 25. rujna 2001., ECHR 2001-IX, stavci 59 – 60.

11 Već i to da su na snazi mjere koje omogućuju provedbu tajnog nadzora komunikacija predstavlja prijetnju nadzora za sve nad kojima bi se mogle primjenjivati, što utječe na slobodu komuniciranja i samo je po sebi zadiranje u prava (čl. 8.) bez obzira na to jesu li mjere primijenjene, vidi npr.: *Klass and others v Germany*, (zahtjev br. 5029/71), 6. rujna 1978., Serija A, br. 28, stavak 41; *Gabriele Weber and Cesar Richard Saravia v Germany*, *op. cit.* u bilj. 10, stavci 77 – 78; *Association for European Integration and Human Rights and Ekimdzhiev v Bulgaria* (zahtjev br. 62540/00), 28. lipnja 2007., stavak 69.

12 *Malone v the United Kingdom*, *op. cit.* u bilj. 10, stavak 84 (detaljnije vidi stavke 56, 83 – 88). Usporedi s presudom Suda u predmetu *P. G. and J. H. v The United Kingdom*, *op. cit.* u bilj. 10, vidi osobito stavke 42 – 51.

13 Što se tiče primjene čl. 8. st. 1. Europske konvencije i odgovarajuće zaštite prava za Sud nije bitno jesu li podaci na ikoji način korišteni. *Copland v The United Kingdom*, *op. cit.* u bilj. 10, stavci 43 – 44.

14 *Leander v Sweden* (zahtjev br. 9248/81), 26. ožujka 1987., Serija A, br. 116, stavak 48. Već i sama pohrana osobnih podataka od strane tijela javne vlasti predstavlja zadiranje u pravo na privatni život, vidi npr. *Amann v Switzerland* (zahtjev br. 27798/95), 16. veljače 2000., ECHR 2000-II, stavak 69.

15 Tako je npr. Sud u predmetu *I v Finland* (zahtjev br. 20511/03), 17. srpnja 2008., utvrdio povredu prava na privatnost zato što u javnoj bolnici nisu poduzete potrebne

U pravu EU-a članak 7. *Povelje temeljnih prava Europske unije* (dalje u tekstu: Povelja)[16], kojim se jamči poštovanje privatnog (i obiteljskog) života, (doma) i komunikacije, ima isto značenje i opseg jamstva iz čl. 8. Europske konvencije.[17] Usko povezano pravo na zaštitu osobnih podataka u pravu EU-a ima status temeljnog samostalnog prava (članak 8. Povelje), a prema tumačenju Europskog suda navedenim se člancima 7. i 8. Povelje jamči pravo na poštovanje privatnog života u vezi s obradom osobnih podataka, koje se tiče svakog podatka koji se odnosi na identificiranog pojedinca ili pojedinca koji može biti identificiran.[18]

U nastavku ćemo se usredotočiti na ispitivanje relevantnog pravnog okvira EU-a i RH u vezi sa zadržavanjem podataka, poglavito s obzirom na utjecaj na privatnost (osobito s obzirom na jamstvo poštovanja prava na privatni život i tajnosti dopisivanja, tj. komuniciranja) i pravo na zaštitu osobnih podataka. U pogledu potonjeg posebno treba skrenuti pozornost na *Konvenciju Vijeća Europe za zaštitu osoba glede automatizirane obrade osobnih podataka* (dalje u tekstu: Konvencija 108)[19], koja je prvi i do danas jedini međunarodnopravni

zaštitne mjere radi sprečavanja neovlaštenog pristupa osjetljivim zdravstvenim podacima, detaljnije vidi osobito u stavcima 35 – 49 presude (http://www.echr.coe.int).

16 Charter of Fundamental Rights of the European Union, OJ C 326, 26. listopada 2012., str. 391 – 407. Povelja danas ima istu pravnu snagu kao i Osnivački ugovori (vidi čl. 6. st. 1. Ugovora o Europskoj uniji – Consolidated version of the Treaty on European Union, OJ C 326, 26. listopada 2012., str. 13) te ona obvezuje institucije, tijela, urede i agencije EU-a, ali i države članice kada primjenjuju pravo EU-a, detaljnije vidi u čl. 51. Povelje.

17 *Explanations relating to the Charter of Fundamental Rights*, OJ C 303, 14. prosinca 2007., str. 17 – 35, na str. 20. Za sudsku praksu Europskog suda vidi npr. C-400/10 PPU *J. McB. v L. E.*, (2010) ECR, I-08965, stavak 53.

18 Detaljnije vidi u C-92/09 i C-93/09 *Volker und Markus Schecke GbR (C-92/09) and Hartmut Eifert (C-93/09) v Land Hessen*, (2010) ECR I-11063. Za definiciju osobnog podatka vidi čl. 2a i recital 26. Direktive 95/46/EZ (te čl. 2. st. 1. točku 1. Zakona o zaštiti osobnih podataka, Narodne novine, br. 106/2012 – pročišćeni tekst) te sudsku praksu Europskog suda, npr.: C-101/01 *Criminal proceedings against Bodil Lindqvist*, (2003) ECR, I-12971, stavak 27, uključivši tumačenje pravne prirode dinamičkih *Internet Protocol* (IP) adresa kao osobnih podataka (barem s obzirom na davatelje usluga pristupa internetu koji mogu identificirati korisnike usluga) u C-70/10 *Scarlet Extended SA v Société Belge des auteurs, compositeurs et éditeurs (SABAM)*, stavak 51. Vidi i C-360/10 *Belgische Vereniging van Auteurs, Componisten en Uitgevers (Sabam) v Netlog NV*, stavak 49. Potonje dvije presude, od 24. studenoga 2011. i 16. veljače 2012. g., nisu još objavljene u ECR-u, tekst dostupan na: http://curia.europa.eu.

19 Convention for the protection of individuals with regard to automatic processing of personal data, 28. siječnja 1981.

instrument u području zaštite osobnih podataka. Republika Hrvatska ratificirala je ovu Konvenciju 2005. g. (zajedno s Dodatnim protokolom)[20] i njezina su temeljna načela ugrađena u *Zakon o zaštiti osobnih podataka* (dalje u tekstu i: ZZOP).[21] Pritom ističemo da se uređenje zaštite osobnih podataka, kako prema Konvenciji 108 tako i prema ZZOP-u, u Republici Hrvatskoj primjenjuje na sve aktivnosti, kako u javnom tako i u privatnom sektoru.[22] U pregledu relevantnih ustavnopravnih jamstava prema domaćem okviru[23] treba istaknuti jamstva poštovanja i ustavnopravne zaštite osobnog (i obiteljskog) života (čl. 35.), slobode i tajnosti dopisivanja i svih drugih oblika općenja (čl. 36.), kao i prava na sigurnost i tajnost osobnih podataka (čl. 37.). Europsku konvenciju Republika Hrvatska ratificirala je 1997. g.[24], a Ustavni je sud u svojoj praksi do danas, pozivajući se i na Europsku konvenciju, ukidao odredbe zakona radi nesuglasnosti s ustavnim načelom vladavine prava te uvjetima dopuštenog ograničavanja zajamčene slobode i tajnosti dopisivanja.[25] Valja skrenuti pozornost i na recentnu odluku Ustavnog suda o ukidanju pojedinih odredbi Zakona o kaznenom postupku zbog nesuglasnosti s jamstvima prava na poštovanje i pravnu zaštitu privatnog života te sigurnosti i tajnosti osobnih podataka – također i u skladu s relevantnom praksom Suda.[26]

---

[20] Zakon o potvrđivanju Konvencije za zaštitu osoba glede automatizirane obrade osobnih podataka i Dodatnog protokola uz Konvenciju za zaštitu osoba glede automatizirane obrade osobnih podataka u vezi nadzornih tijela i međunarodne razmjene podataka, Narodne novine, Međunarodni ugovori, br. 4/2005.

[21] Zakon o zaštiti osobnih podataka, Narodne novine, br. 106/2012 – pročišćeni tekst.

[22] Jedino isključeno područje je obrada koju fizičke osobe obavljaju samo za osobnu primjenu ili potrebe kućanstva. Čl. 3. st. 4. ZZOP-a; za Konvenciju 108 vidi čl. 3. st. 2. ZZOP-a i čl. 3. Zakona o potvrđivanju Konvencije 108, *op. cit.* u bilj. 20, u vezi s čl. 3. st. 2a te Konvencije, a za relevantne izjave država pa tako i RH vidi: Council of Europe, *List of declarations made with respect to treaty No. 108*, dostupno pretragom na: http://conventions.coe.int/ (11. ožujka 2013.). S druge strane, za propisanu mogućnost ograničenja *pojedinih odredbi* i uvjete vidi čl. 9. st. 1. – 2. u vezi s čl. 5., 6. i 8. Konvencije 108 te čl. 23. st. 1. u vezi s čl. 9. i 19. ZZOP-a.

[23] Ustav Republike Hrvatske, Narodne novine, br. 85/2010 – pročišćeni tekst.

[24] Zakon o potvrđivanju Konvencije za zaštitu ljudskih prava i temeljnih sloboda i Protokola br. 1., 4., 6., 7. i 11. uz Konvenciju za zaštitu ljudskih prava i temeljnih sloboda, Narodne novine, Međunarodni ugovori, br. 18/1997 (pročišćeni tekst: Narodne novine, Međunarodni ugovori, br. 6/1999 i 8/1999).

[25] Čl. 3. i čl. 36. st. 2. Ustava Republike Hrvatske; vidi npr. Odluku i Rješenje Ustavnog suda RH br. U-I-985/1995, U-I-792/1998, U-I-1088/1998, U-I-123/1999 od 23. veljače 2000. (Narodne novine, br. 29/2000).

[26] Odluka Ustavnog suda Republike Hrvatske br. U-I-448/2009 od 19. srpnja 2012., Narodne novine, br. 91/2012.

Razvoj domaćeg zakonodavnog okvira kako u općem području zaštite prava pojedinca u vezi s obradom osobnih podataka, a poglavito zaštite prava na privatnost, tako i u području zaštite tih prava u sektoru elektroničkih komunikacija pod osobito je snažnim utjecajem *acquisa*. Tako su odredbe *Direktive 95/46/EZ o zaštiti pojedinaca u pogledu obrade osobnih podataka i njihovog slobodnog protoka* (dalje u tekstu: Direktiva 95/46/EZ) koja ima opće područje primjene[27] u određenoj mjeri transponirane u ZZOP, dok su odredbe *Direktive 2002/58/EZ o obradi osobnih podataka i zaštiti privatnosti u sektoru elektroničkih komunikacija* (dalje u tekstu: Direktiva o e-privatnosti)[28] implementirane u *Zakonu o elektroničkim komunikacijama* (dalje u tekstu i: ZEK).[29]

Mjere zadržavanja koje sagledavamo u radu uključuju obvezno prikupljanje i pohranu niza prometnih podataka, ali i podataka o lokaciji te identifikacijskih podataka, koji se odnose na sve korisnike usluga. Iako se zbog posebnije osjetljivosti ne nalaže pohrana podataka koji otkrivaju sadržaj komunikacije, navedeni prometni i drugi podaci također su osjetljivi jer sadržavaju informacije koje se tiču privatnog života i prava na poštovanje tajnosti komuniciranja pojedinaca.[30] Osobito imamo li u vidu akumulaciju takvih podataka u duljem razdoblju i mogućnosti tehnologija te postupaka analiza i profiliranja, na temelju ovih podataka je, naime, moguće dobiti uvid u brojne aspekte privatnog života osoba na koje se odnose (društveni život, interesi, kretanje – mobilna telefonija i dr.[31]).

---

[27] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23. studenoga 1995., str. 31 – 50. Detaljnije u pogledu općeg područja primjene ove Direktive vidi u čl. 3. i recitalu 27.

[28] Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector, OJ L 201, 31. srpnja 2002., str. 37 – 47. Zadnji je put ona mijenjana 2009. g. (Direktivom 2009/136/EZ, OJ L 337, 18. prosinca 2009., str. 11 – 36).

[29] Zakon o elektroničkim komunikacijama, Narodne novine, br. 73/2008, 90/2011 i 133/2012.

[30] Recital 17. Direktive 97/66/EZ i recital 26. Direktive o e-privatnosti. Komunikacija može uključivati bilo koje informacije o imenu, broju ili adresi koje pruža pošiljatelj komunikacije ili korisnik priključka s ciljem prijenosa komunikacije, a prometni podaci mogu uključivati bilo koje pretvaranje ovih informacija putem mreže preko koje se odvija komunikacija u svrhu prijenosa (recital 15. Direktive o e-privatnosti).

[31] Već i jednostavnija analiza podataka o pozivima omogućuje utvrđivanje detalja o društvenom životu osobe (npr. krug osoba s kojima je u bliskom odnosu), a osim podataka o pozivanim brojevima dodatni detalji mogu se otkriti analizom drugih

Budući da je obvezno preventivno zadržavanje podataka koji se odnose na komunikaciju svih korisnika usluga (i na njihov identitet) na određeni rok mjera kojom se snažno zadire u zajamčena prava građana na poštovanje privatnog života i tajnosti komuniciranja, kao i prava na zaštitu osobnih podataka, kod uvođenja i uređenja takve mjere u domaćem pravnom sustavu mora se pristupati s osobitom pažnjom. Sagledavajući izvore prava EU-a, uređenje takvih mjera u skladu s propisima predstavlja iznimku od *obveze čuvanja tajnosti elektroničkih komunikacija*[32] *i pripadajućih prometnih podataka* u javnim komunikacijskim mrežama i javno dostupnim komunikacijskim uslugama, čije je temeljno pravilo zabrana slušanja, prisluškivanja, pohranjivanja, tj. svakog presretanja ili nadzora nad ovim podacima.[33] Takvom mjerom izuzimaju se od primjene i posebna pravila o *obradi prometnih podataka* koji se odnose na pretplatnike i korisnike usluga (koja su sama po sebi propisana iznimka od ranije navedene obveze čuvanja tajnosti komunikacija i prometnih podataka), s posebno utvrđenim zaštitnim mjerama (kontrola pristupa, tj. ovlaštenih osoba za pristup obradi podataka, ograničenja opsega poslova i roka čuvanja, tj. obrade s obzirom na dopuštenu svrhu obrade). Naime, prema ovim je pravilima temeljna obveza operatora brisanje ili anonimizacija navedenih podataka čim oni više nisu potrebni radi prijenosa komunikacije. Tipična, ali ne i jedina propisana iznimka od takve je obveze pohrana (i obrada) onih prometnih podataka *koji su potrebni za obračun i naplatu* troškova usluge i koji se u takvom slučaju u tu svrhu smiju sačuvati, samo za ograničeni rok (zastara potraživanja) te uz ob-

podataka u vezi s pozivima (npr. vrijeme poziva, trajanje, učestalost pozivanja nekih brojeva). Omogućuje se uvid i u različite interese i sklonosti pozivatelja, kao npr. potrošačka sklonost, sklonost sudjelovanju u igrama na sreću, traženju savjeta (astrologija, tarot) i dr., a pozivanje specijaliziranih brojeva (radi npr. savjetovanja o zdravlju ili psihološka i bračna savjetovališta) omogućuje profiliranje i s obzirom na najintimnije aspekte osobnosti pozivatelja. Detaljnije u tom smislu vidi presudu njemačkog Saveznog ustavnog suda od 2. ožujka 2010.: BVerfG, 1 BvR 256/08, dostupno pretragom na: http://www.bverfg.de/entscheidungen/.

[32] Komunikacija je svaka obavijest koja je razmijenjena ili prenesena između konačnog broja sudionika putem javno dostupne elektroničke komunikacijske usluge (ovdje u pravilu ne ulaze informacije koje se prenose javnosti elektroničkom komunikacijskom mrežom u sklopu djelatnosti radija i televizije, osim ako se mogu povezati s odredivim pretplatnikom ili korisnikom usluga koji ih prima). Prometni podaci definiraju se kao bilo koji podaci koji se obrađuju radi prijenosa komunikacije elektroničkom komunikacijskom mrežom ili u svrhu obračuna i naplate troškova. Vidi čl. 2. st. 1. točke 24. i 55. ZEK-a i čl. 2. st. 2 b i d Direktive o e-privatnosti.

[33] Detaljnije vidi u čl. 100. ZEK-a i čl. 5. Direktive o e-privatnosti.

vezu primjene zaštitnih mjera kako bi se spriječio neovlašteni pristup, tj. bilo koja nedopuštena obrada takvih podataka.[34]

Uz raniju napomenu o zadržavanju podataka kao iznimci od zajamčenih prava korisnika i povezanih posebnih obveza operatora (ali i opće zabrane nadzora nad podacima), važno je imati na umu uvjete koje države članice EU-a moraju zadovoljiti prilikom propisivanja takvih mjera u unutarnjem pravu, tj. kod utvrđivanja mjera kojima se ograničavaju pojedina prava i obveze kako je to predviđeno Direktivom o e-privatnosti.[35] Napominjemo da se ti uvjeti, na koje upućujemo u nastavku, *ne primjenjuju* na podatke koji se moraju zadržati prema Direktivi o zadržavanju podataka[36] – sustav obveznog zadržavanja koji se putem potonje Direktive želi harmonizirati unutar EU-a analizirat ćemo dalje u radu.

Mjera (kojom se ograničuju relevantna prava korisnika i obveze operatora) mora biti *potrebna, odgovarajuća i razmjerna u demokratskom društvu radi zaštite nacionalne i javne sigurnosti, obrane, sprečavanja istrage, otkrivanja i progona kaznenih djela ili neovlaštenog korištenja elektroničkog komunikacijskog sustava*, kako je to utvrđeno čl. 13. st. 1. Direktive 95/46/EZ.[37] Ona mora biti usklađena i s općim načelima prava EU-a, uključujući načela iz čl. 6. Ugovora o Europskoj uniji (dalje u tekstu: UEU)[38] koja obuhvaćaju i jamstva iz Europske konvencije, a prema tome i ograničenja prava u skladu s tumačenjima Suda.[39] S ovime u vidu

---

[34] Detaljnije, kao i za druge izričito propisane iznimke i uvjete koji se moraju ispuniti kako bi takva obrada prometnih podataka bila zakonita, vidi u čl. 102. ZEK-a, usporedi s čl. 6. Direktive o e-privatnosti.

[35] Čl. 15. st. 1. Direktive o e-privatnosti.

[36] Vidi čl. 11. i recital 12. Direktive o zadržavanju podataka i čl. 15. st. 1a Direktive o e-privatnosti.

[37] Za tumačenje vidi osobito: C-275/06 *Productores de Música de España (Promusicae) v Telefónica de España SAU*, (2008) ECR, I-00271; C-461/10 *Bonnier Audio AB and Others v Perfect Communication Sweden AB* (presuda od 19. travnja 2012. g. nije još objavljena u ECR-u, tekst je dostupan na: http://curia.europa.eu).

[38] UEU, *op. cit.* u bilj. 16, vidi čl. 6. st. 1. i. st. 3.

[39] Vidi čl. 8. st. 2. Europske konvencije te čl. 15. st. 1. (i čl. 1. st. 3.) i recital 11. Direktive o e-privatnosti. Za primjer primjene Europske konvencije vidi *S. and Marper v The United Kingdom* (zahtjevi br. 30562/04 i 30566/04), 4. prosinca 2008., ECHR-2008. Podnositelji zahtjeva osporavali su odredbe engleskog zakona o policiji prema kojima je policija odbila uništiti/izbrisati prikupljene otiske prstiju, uzorke stanica i profil DNK-a nakon što je protiv jednog podnositelja obustavljen kazneni postupak, dok je drugi oslobođen optužbe (jedan podnositelj bio je i maloljetnik). Zakonom je bilo propisano trajno, bezuvjetno i neograničeno zadržavanje podataka (bez obzira na vrstu i težinu djela, ishod kaznenog postupka, dob osoba). Kako je

bitno je imati na umu članak 8. st. 2. Europske konvencije i njegova tumačenja u praksi Suda. Prema navedenom javna vlast neće se miješati u ostvarivanje zajamčenih prava (npr. pravo na privatni život), osim u skladu sa zakonom i ako je to nužno u demokratskom društvu radi interesa državne sigurnosti, javnog reda i mira, gospodarske dobrobiti zemlje, sprečavanja nereda ili zločina, zaštite zdravlja ili morala ili radi zaštite prava i sloboda drugih. Ograničenje mora biti u skladu sa zakonom koji mora biti dostupan i predvidljiv, tj. dovoljno precizan i jasan da se osobe mogu po njemu ponašati. Ono mora biti nužno u demokratskom društvu i mora se provoditi isključivo radi ispunjenja legitimnog cilja. Mjerom se mora zadovoljiti vrlo važna, neodgodiva socijalna potreba da se ispuni legitimni cilj, pri čemu ona mora biti razmjerna u odnosu na taj cilj pa tako uvijek treba razmotriti može li se taj cilj postići mjerom kojom se u manjem opsegu zadire u temeljno pravo. Sagledaju li se navedeni uvjeti u odnosu s uvjetima ograničenja relevantnih prava prema Povelji[40], razvidno je kako oni u bitnom odgovaraju ograničenjima koja se toleriraju u od-

takva mjera miješanje javne vlasti u pravo na privatni život, Sud je dalje razmatrao jesu li zadovoljeni kriteriji čl. 8. st. 2. Europske konvencije. Utvrdio je da je zaštita osobnih podataka od temeljne važnosti za uživanje prava pojedinca na privatni i obiteljski život. U domaćem pravnom okviru moraju se osigurati odgovarajuće zaštitne mjere radi sprečavanja svakog korištenja osobnih podataka koje bi moglo biti neusklađeno s jamstvima čl. 8, a potreba za ovime to je veća ako je riječ o automatiziranoj obradi. Domaće pravo osobito treba osigurati da su podaci relevantni i nisu suvišni u odnosu na svrhe radi kojih se pohranjuju, da se ne čuvaju u obliku koji dopušta identifikaciju ispitanika dulje nego je potrebno za svrhu za koju su pohranjeni te osigurati jamstva učinkovite zaštite zadržanih podataka od nedopuštenog korištenja i zlouporabe (stavci 103 – 104 presude). Zakonom se mora osigurati pravna zaštita od samovolje i prema tome utvrditi, s dovoljnom jasnoćom, opseg diskrecije za nadležna tijela i način izvršavanja: "[…] bitno je i u ovome kontekstu, kao i kod telefonskog prisluškivanja, tajnog nadzora i skrivenog prikupljanja informacija, imati jasna, detaljna pravila kojima se uređuje opseg i primjena mjera, kao i minimalne zaštitne mjere u pogledu, *inter alia*, trajanja, pohrane, korištenja, pristupa od strane trećih, postupaka radi očuvanja cjelovitosti i povjerljivosti podataka i postupaka oko njihovog uništavanja, čime se pružaju dovoljna jamstva u odnosu na rizik od zlouporabe i samovolje […]" Neslužbeni prijevod, stavak 99 (vidi i sudsku praksu na koju Sud upućuje). Sud nije ovdje ulazio u dublju analizu ovih kriterija kvalitete zakona, već je utvrdio da su ta pitanja usko povezana sa širim pitanjem je li zadiranje potrebno u demokratskom društvu te nastavio analizu istog (vidi stavke 105. – 126.). Na ovaj predmet recentno je upozorio i Ustavni sud RH prilikom ukidanja relevantnih odredbi Zakona o kaznenom postupku, *op. cit.* u bilj. 26, točke 158. – 158.4. (vidi i točke 101. – 101.2.).

[40] Ovo uz napomenu o području primjene Povelje, *op. cit.* u bilj. 16.

nosu na čl. 8. Europske konvencije.[41] Naime, prema Povelji svako ograničenje prava mora biti propisano zakonom (na jasan i predvidljiv način) i poštovati njegovu bit te, u skladu s načelom razmjernosti[42], mora biti nužno i takvo da se njime doista može ostvariti cilj od javnog interesa koji priznaje EU ili potreba zaštite prava i sloboda drugih osoba.[43] Osim toga, treba imati na umu i da se kod provedbe prava EU-a u unutarnje pravo te u slučaju međuodnosa različitih temeljnih prava i sloboda moraju primjenjivati tumačenja Europskog suda sukladno njegovoj sudskoj praksi.[44]

Uz analizirane obveze kod propisivanja domaćih mjera kojima se ograničuju relevantna prava korisnika (pa tako i mjera zadržavanja podataka u elektroničkim komunikacijama u druge svrhe od onih propisanih Direktivom o zadržavanju podataka), treba obratiti pozornost i na novija (2009.) pravila Direktive o e-privatnosti u svrhu transparentnosti, ali i kontrole pravilnosti postupaka dostave podataka korisnika (prema navedenim domaćim propisi-

[41] C-92/09, *op. cit*. u bilj. 18, osobito stavci 47 – 52. Vidi i čl. 8. st. 2., čl. 52. st. 1. i st. 3. te čl. 53. Povelje.

[42] Načelo razmjernosti (proporcionalnosti) nalaže da mjere koje se provode putem akata EU-a trebaju biti odgovarajuće za postizanje cilja koji se želi ispuniti i da ne idu dalje od onog što je potrebno za to ispunjenje. Vidi npr. odluku Europskog suda u C-92/09, *op. cit*. u bilj. 18, osobito stavak 74. Detaljnije razrađeno u praksi Europskog suda ovo načelo zahtijeva da mjere koje usvajaju institucije EU-a ne prelaze granice onoga što je prikladno i nužno da se postignu ciljevi koje zakonodavstvo u pitanju želi legitimno postići, a kada postoji izbor između više odgovarajućih mjera, potrebno je prikloniti se najmanje otegotnoj, s time da uzrokovani nedostaci (nepogodnosti) ne smiju biti nerazmjerni ciljevima koji se žele postići, vidi: C-283/11 *Sky Österreich GmbH v Österreichischer Rundfunk*, stavak 50 (presuda od 22. siječnja 2013. g. nije još objavljena u ECR-u, tekst dostupan na: http://curia.europa.eu). Ako je u pitanju više temeljnih prava i sloboda koje štiti pravni sustav EU-a, procjenu moguće nerazmjerne prirode odredbe prava EU-a treba provesti s ciljem da se pomire zahtjevi zaštite tih različitih prava i sloboda i osiguravanja pravedne ravnoteže između njih. *Ibid.*, stavak 60.

[43] Vidi čl. 52. st. 1. Povelje i strategiju Komisije za učinkovitu provedbu Povelje: *Communication from the Commission. Strategy for the effective implementation of the Charter of Fundamental Rights by the European Union*, Brussels, 19. listopada 2010., COM (2010) 573/4, osobito kontrolnu listu na str. 5.

[44] Države članice moraju se oslanjati na tumačenje akata EU-a na način koji dopušta pravednu ravnotežu između različitih temeljnih prava. Osim toga, sudovi i tijela vlasti dužni su kod provedbe mjera putem kojih se ovi propisi prava EU-a transponiraju, tumačiti unutarnje pravo na dosljedan način u odnosu na iste, ali i osigurati da se ne oslanjanju na tumačenje tih propisa EU-a koje dovodi do sukoba s ovim temeljnim pravima ili drugim općim načelima prava EU-a, kao što je načelo razmjernosti. Vidi C-275/06, *op. cit.* u bilj. 37, stavak 70.

ma). Naime, države članice EU-a dužne su osigurati da davatelji javnih komunikacijskih mreža i/ili javno dostupnih elektroničkih komunikacijskih usluga uspostave interne postupke kada odgovaraju na zahtjeve za pristup osobnim podacima korisnika, kao i njihovu obvezu da *na zahtjev ovlaštenog domaćeg tijela* dostave podatke o postupcima, broju zaprimljenih zahtjeva, pravnoj osnovi na koju se pozivalo kod traženja pristupa podacima te odgovoru operatora.[45]

Na kraju ovog pregleda skrećemo pažnju na novine u pravu EU-a koje su bitne za daljnju analizu aktualnih pitanja oko uređenja mjera zadržavanja. Naime, države članice nisu prema ranijoj podjeli na stupove morale implementirati Direktivu 95/46/EZ i Direktivu o e-privatnosti u područjima izvan prvog stupa (osobito se to odnosi na javnu i državnu sigurnost, obranu, aktivnosti države u kaznenopravnom području).[46] Uz stupanje na snagu Lisabonskog ugovora i ukidanje stupova, Ugovorom o funkcioniranju EU-a (dalje u tekstu: UFEU) utvrđena je nova pravna osnova za uređenje zaštite osobnih podataka u EU-u.[47] Sukladno tome danas su u tijeku zakonodavni postupci povodom prijedloga *Opće uredbe o zaštiti osobnih podataka*[48], ali i *Direktive o za-*

[45] Čl. 15. st. 1b Direktive o e-privatnosti. Prema prvim prijedlozima Komisije i Parlamenta ovdje je bila predviđena stroža obveza operatora da dostavljaju nadzornim tijelima za zaštitu osobnih podataka podatke o svakom zahtjevu za osobnim podacima, pravnoj osnovi i proceduri te ovlasti nadzornih tijela da obavijeste sud ako smatraju da nije postupano u skladu s domaćim pravom. *Amended proposal for a Directive of the European Parliament and of the Council Amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sectors and Regulation (EC) No 2006/2004 on consumer protection cooperation* /* COM/2008/0723 final - COD 2007/0248 */ (vezano za amandman 136).

[46] Vidi čl. 3. st. 2. alineju 1 Direktive 95/46/EZ i čl. 1. st. 3. Direktive o e-privatnosti.

[47] Detaljnije vidi u čl. 16. UFEU-a – Consolidated version of the Treaty on the Functioning of the European Union, OJ C 326, 26. listopada 2012., str. 47, kao i izjave uz Lisabonski ugovor (OJ C 83, 30. ožujka 2010., str. 347) i to: a) Izjavu 21 o tome da nova pravna osnova (čl. 16. UFEU-a) ne isključuje mogućnost uspostave pravila o zaštiti podataka u specifičnim područjima pravosudne suradnje u kaznenim stvarima i policijske suradnje (Declaration on the protection of personal data in the fields of judicial cooperation in criminal matters and police cooperation); b) Izjavu 20 o potrebi uzimanja u obzir značajki posljedica novih pravila o zaštiti podataka prema čl. 16. UFEU-a za nacionalnu sigurnost (Declaration on Article 16 of the Treaty on the Functioning of the European Union).

[48] European Commission, *Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation*), COM (2012) 11 final, 2012/0011 (COD), 25. siječnja 2012.

štiti pojedinaca u vezi s obradom osobnih podataka od strane nadležnih tijela u svrhe sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili provedbe kaznenopravnih sankcija, te o slobodnom kretanju tih podataka.[49] Potonjom Direktivom zamijenila bi se *Okvirna odluka Vijeća 2008/977/JHA*[50] koja bi se osim na prekograničnu razmjenu osobnih podataka unutar EU-a (kako je to danas prema Okvirnoj odluci) primjenjivala i na relevantnu obradu *unutar država članica*. S time u vidu kao i, osobito, jamstvom članka 8. Povelje na koje smo ranije upozorili (ali i pojednostavljenim donošenjem propisa o određenim pitanjima policijske i pravosudne suradnje[51]) može se pretpostaviti da će se budući okvir EU-a o zaštiti podataka u određenoj mjeri primjenjivati i u području zadržavanja podataka u elektroničkim komunikacijama od strane nadležnih tijela država članica koja tim podacima pristupaju.

2.2. Zadržavanje podataka u pravu EU-a

Cilj utvrđivanja obveza zadržavanja podataka u elektroničkim komunikacijama prema Direktivi osiguravanje je dostupnosti tih podataka u svrhu istrage, otkrivanja i progona (ne i sprečavanja[52]) teških kaznenih djela[53], s time da se pojam i okolnost teških kaznenih djela ostavlja na utvrđivanje državama u skladu s unutarnjim pravom.[54] Podaci koji se moraju zadržavati uključuju prometne

---

[49] *Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data*, COM/2012/010 final, 2012/0010 (COD), 25. siječnja 2012. Skrećemo pažnju na predloženu pravnu osnovu (čl. 16. st. 2. UFEU-a u vezi s čl. 39. UEU-a), kao i na to da se ova Direktiva ne bi primjenjivala na pitanja obrade u okviru aktivnosti izvan područja primjene prava EU-a, osobito u vezi s nacionalnom sigurnosti (čl. 2. st. 3a).

[50] Council Framework Decision 2008/977/JHA of 27.11.2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, OJ L 350, 30. prosinca 2008., str. 60 – 71.

[51] Redoviti zakonodavni postupak – osobito vidi čl. 87. st. 2. UFEU-a.

[52] Iz konačnog teksta, naime, izbačen je prijedlog da se podaci zadrže i radi *sprečavanja* teških kaznenih djela.

[53] Čl. 1. st. 1. Direktive o zadržavanju podataka.

[54] U recitalu 9. nužnost zadržavanja argumentira se na način da se ono u nekoliko država članica pokazalo potrebnim i učinkovitim istražnim sredstvom, osobito oko teških kaznenih djela kao što su organizirani kriminal i terorizam, ali u relevantnom članku ne nabrajaju se primjeri (čl. 1. st. 1.) kojima se zamijenila ranija verzija istog članka koja je sadržavala te primjere, vidi *op. cit*. u bilj. 1 (čl. 1. st. 1.).

podatke (i podatke o lokaciji) te podatke nužne za identificiranje pretplatnika ili registriranog korisnika[55], tj. podatke koji su potrebni za: a) otkrivanje i identifikaciju izvora komunikacije; b) identifikaciju odredišta komunikacije; c) identifikaciju datuma, vremena i trajanja komunikacije; d) određivanje vrste komunikacije; e) identifikaciju sredstva za komunikaciju te za f) otkrivanje lokacije opreme za pokretnu komunikaciju (sve u fiksnoj i mobilnoj telefoniji kao i za internetski pristup, e-poštu te internetsku telefoniju). Ne nalaže se zadržavanje podataka u vezi s pozivima koji nisu spojeni, a za neuspješne pokušaje poziva[56] pravilo je da ako se oni do Direktive nisu pohranjivali (u okviru pružanja usluga), tada se za državu ne uspostavlja obveza njihove pohrane.[57] Nema propisane obveze zadržavanja podataka koji se odnose na sadržaj komunikacije, uključivo informacija koje se pregledavaju tijekom korištenja elektroničke komunikacijske mreže (npr. posjećivane mrežne stranice).[58]

Države su dužne jednom godišnje dostaviti Europskoj komisiji statistiku o zadržavanju, s podacima o slučajevima kada su podaci dostavljeni nadležnim tijelima, razdoblju od zadržavanja do prijenosa te kada se zahtjevu nije moglo udovoljiti. Naime, postupak izvješćivanja i podaci država nužni su radi ocjene potrebe eventualnih izmjena Direktive, poglavito oko opsega i roka zadržavanja podataka.[59] Posebno treba obratiti pažnju na *minimalna sigurnosna načela* koja operatori moraju osigurati, pa tako zadržani podaci moraju biti jednake kvalitete i na njih se moraju primjenjivati iste sigurnosne i zaštitne mjere kao i na podatke u mreži. Također se moraju provoditi tehničke i organizacijske mjere kako bi se zadržani podaci zaštitili od slučajnog ili nezakonitog uništenja, slučajnog gubitka ili izmjene, ili od neovlaštenog ili nezakonitog pohranjivanja, obrade, pristupa ili otkrivanja. Nadalje, mora se osigurati da samo ovlašteno osoblje može pristupiti podacima, a osim toga podaci se moraju *uništiti po isteku roka zadržavanja* (uz iznimku onih kojima se pristupilo i sačuvani su za potrebe nadležnih tijela). Uz navedene je mjere važna obveza država da osiguraju *neovisan nadzor* nad provedbom odgovarajućih domaćih odredbi, koji mogu obavljati domaća tijela za zaštitu osobnih podataka.[60] Napominjemo da se na zadržane podatke u cijelosti primjenjuju odredbe Direktive 95/46/EZ i Direktive o e-pri-

[55] Čl. 5. Direktive o zadržavanju podataka.

[56] Vidi čl. 2. točku f Direktive o zadržavanju podataka.

[57] Vidi čl. 3. st. 2. kao i recital 12. Direktive o zadržavanju podataka.

[58] Vidi čl. 5. st. 2. u vezi sa čl. 1. st. 2. Direktive o zadržavanju podataka.

[59] Vidi čl. 10. i čl. 14. Direktive o zadržavanju podataka.

[60] Vidi čl. 9. u vezi s čl. 7. Direktive o zadržavanju podataka i čl. 28. Direktive 95/46/EZ.

vatnosti, kao i Konvencije 108 i Konvencije o kibernetičkom kriminalu[61] te se mora osigurati primjena domaćih mjera usvojenih prema Direktivi 95/46/EZ[62], kao i kažnjavanje namjernog neovlaštenog pristupa (ili prijenosa) zadržanim podacima i to sankcijama koje su učinkovite, razmjerne i odvraćajuće.[63]

Naposljetku napominjemo da Direktiva ne uređuje pristup podacima[64], ali nalaže usvajanje mjera kojima će se osigurati da se zadržani podaci daju samo nadležnim tijelima u posebnim slučajevima, u skladu s domaćim pravom. Tako Direktiva, u mjeri koja u bitnom odgovara ranije analiziranim uvjetima ograničenja prava prema Direktivi o e-privatnosti, nalaže *državama da utvrde postupak i uvjete koji se moraju poštovati kako bi se podacima pristupilo u skladu sa zahtjevima nužnosti i razmjernosti, uz poštovanje prava EU-a i međunarodnog prava te osobito Europske konvencije u skladu s praksom Europskog suda za ljudska prava*.[65]

2.3. Zadržavanje podataka u domaćem pravu

Odredbe Direktive implementirane su u Zakonu o elektroničkim komunikacijama[66] 2008. g., s temeljnom obvezom operatora javno dostupnih elektroničkih komunikacijskih usluga i operatora javnih komunikacijskih mreža[67] na zadržavanje podataka na rok od 12 mjeseci od obavljene komunikacije. Ujedno su propisane prekršajne sankcije u slučaju neispunjavanja relevantnih obveza operatora, što se smatra teškom povredom ZEK-a.[68] Bitno je imati na umu da je u domaćem pravnom okviru danas također na snazi još i ranije uvedena mjera obveznog preventivnog zadržavanja podataka građana (dakle, neovisno o Direktivi) sukladno *Zakonu o sigurnosno-obavještajnom sustavu Republike Hrvatske* (dalje u tekstu: ZSOS)[69] i na temelju njega usvojenoj *Uredbi Vlade RH o obvezama iz područja nacionalne sigurnosti Republike Hrvatske za pravne i fizičke*

---

61 Detaljnije vidi osobito u čl. 7. i čl. 13. kao i recitalima 15. – 20. Direktive o zadržavanju podataka.

62 U relevantnom poglavlju III. Direktive 95/46/EZ predviđa se sudska zaštita prava i pravo na zahtjev za naknadu štete te se uređuju pitanja odgovornosti za povrede propisa usvojenih na temelju ove Direktive.

63 Čl. 13. Direktive o zadržavanju podataka. Vidi i recitale 17. – 19. Direktive.

64 Vidi pojašnjenja u recitalu 25. Direktive u vezi s čl. 3. st. 2., 1. al. Direktive 95/46/EZ.

65 Čl. 4. Direktive o zadržavanju podataka. Vidi i recital 17. Direktive.

66 Čl. 109. - 110. ZEK-a.

67 Za definicije relevantnih pojmova u ZEK-u vidi čl. 2. ovog zakona.

68 Detaljnije vidi u čl. 119. st. 1. točkama 57. – 58., čl. 119. st. 2. – 7. ZEK-a.

69 Narodne novine, br. 79/2006 i 105/2006. Vidi čl. 19. st. 5. u vezi s čl. 18. st. 1. ZSOS-a.

osobe u telekomunikacijama (dalje u tekstu: Uredba (2008.)).[70] Analiza rješenja obveznog zadržavanja podataka u elektroničkim komunikacijama u domaćem pravnom okviru u ovome radu nužno uključuje i odredbe navedenih propisa[71], čemu u prilog govori i njihova povezanost s rješenjima ZEK-a, što ćemo pojasniti kroz primjere u nastavku.

Uvodno treba istaknuti da je opseg adresata obveze zadržavanja prema ZSOS-u širi i ponešto drukčiji od onog utvrđenog ZEK-om (koji je to propisao sukladno Direktivi). Naime, prema ZSOS-u ovdje je riječ o svim pravnim i fizičkim osobama koje raspolažu javnom telekomunikacijskom mrežom i pružaju javne telekomunikacijske usluge i usluge pristupa u RH[72], a te se osobe pobliže određuju Uredbom (2008.).[73] Tom Uredbom utvrdio se niz obveza ovih adresata u području nacionalne sigurnosti (o čemu govori i sam naziv Uredbe), koje se odnose na funkciju tajnog nadzora telekomunikacija. Zakonom (ZSOS) se propisuju samo *kategorije mjera nadzora* i na osnovi toga zakonski uvjeti kada se pojedina mjera smije provesti. Drugim riječima, Zakonom (ZSOS) se nije utvrdio i sam *sadržaj, tj. opis konkretnih radnji, kojima se pojašnjava bit pojedine vrste nadzorne mjere,* već je to zakonodavac ostavio da se propiše Uredbom (2008.) ("Funkcionalni zahtjevi"), što smatramo osobito problematičnim rješenjem.

Prema tekstu Uredbe (2008.) proizlazi da je mjera obveznog preventivnog zadržavanja podataka u elektroničkim komunikacijama (bez sadržaja) uključena u odredbama o *mjeri tajnog nadzora podataka o telekomunikacijskom prometu.*[74]

---

[70] Narodne novine, br. 64/2008. Vidi čl. 20. Uredbe (2008.). Zadržavanje podataka bilo je propisano ranijom Uredbom (Narodne novine, br. 83/2003) čiju je ustavnost i zakonitost osporavao pučki pravobranitelj, ali o tome nije odlučeno dok ona nije stavljena izvan snage donošenjem Uredbe (2008.) po osnovi novog zakona (ZSOS). Zahtjev za ocjenu suglasnosti s Ustavom i zakonom primarno je, ali ne i isključivo, temeljen na argumentu da je ranija Uredba donesena bez zakonske osnove, detaljnije vidi u Malčić, J. – pučki pravobranitelj, *Zahtjev Ustavnom sudu Republike Hrvatske, br. P.P.R.-11/05-1*, 23. veljače 2005., http://www.ombudsman.hr/ (8. prosinca 2012.).

[71] Ovo uz napomenu da opseg rada ne dopušta detaljnu analizu svih domaćih propisa koji dolaze u obzir kod razmatranja ove problematike.

[72] Čl. 19. st. 5. u vezi s čl. 18. st. 1. ZSOS-a. Vidi i čl. 20. st. 1. ZSOS-a.

[73] Telekomunikacijski i mrežni operatori, davatelji javnih telekomunikacijskih usluga i davatelji pristupa telekomunikacijskim mrežama, internetu ili drugim računalnim mrežama u smislu Uredbe te druge pravne i fizičke osobe određene zakonom. Čl. 2. Uredbe (2008.). Navedeni se pojmovi pretežito definiraju ovom Uredbom; usporedi pojmove i značenja u čl. 3. Uredbe (2008.) s relevantnom terminologijom prema ZEK-u (čl. 2.).

[74] Čl. 20. – 26. Uredbe (2008.). Skrećemo pažnju i na druge odredbe iz kojih je tako-

Gore navedeni adresati dužni su, naime, zadržavati podatke o telekomunikacijskom prometu ostvarenom unutar i preko vlastitih telekomunikacijskih kapaciteta te osigurati da zadržani podaci *budu raspoloživi* Operativno-tehničkom centru za nadzor telekomunikacija (dalje u tekstu: OTC)[75] *putem propisanog tehničkog sučelja za rok od zadnjih 12 mjeseci.*

Što se tiče uvjeta za provedbu same mjere *tajnog nadzora podataka o telekomunikacijskom prometu*, tu mjeru prema ZSOS-u odobravaju ravnatelji sigurnosno-obavještajnih agencija.[76] U svrhu osiguravanja zaštite jamstava prava i sloboda građana smatramo nužnim razmotriti uspostavu neovisne, tj. sudske kontrole nad pristupom preventivno zadržanim podacima korisnika usluga u elektroničkim komunikacijama za rok od 12 mjeseci. Osim toga treba obratiti pažnju i na pojedine druge odredbe Uredbe (2008.) iz kojih proizlazi uređivanje obveznog preventivnog zadržavanja podataka korisnika za rok od 12 mjeseci (npr. podaci o zemljopisnoj, fizičkoj ili logičkoj lokaciji sredstava za komuniciranje u slučaju postojanja telekomunikacijske aktivnosti[77], podaci radi identifikacije korisnika i usluga[78]).

đer razvidno utvrđivanje obveznog zadržavanja pojedinih vrsti podataka na 12 mjeseci, poglavito vidi čl. 27. st. 2. i čl. 33. Uredbe (2008.).

75 OTC je osnovan temeljem ZSOS-a radi obavljanja aktivacije i upravljanja mjerom tajnog nadzora telekomunikacijskih usluga, djelatnosti i prometa te ostvarivanja operativno-tehničke koordinacije između osoba koje raspolažu javnom telekomunikacijskom mrežom i pružaju javne telekomunikacijske usluge i usluge pristupa u RH i ovlaštenih tijela za primjenu mjera tajnog nadzora telekomunikacija sukladno tom Zakonu i Zakonu o kaznenom postupku, vidi čl. 18. ZSOS-a i čl. 3. Uredbe (2008.) kao i čl. 9. – 11. i čl. 39. Uredbe (2008.).

76 Uvjet je pisani i obrazloženi nalog u propisanom djelokrugu, detaljnije vidi u čl. 38. ZSOS-a. Takav postupak propisan je i za mjeru tajnog nadzora lokacije pri kojoj po Uredbi također dolazi do mogućnosti korištenja zadržanih podataka (o lokaciji uređaja) s obzirom na propisanu obvezu da se OTC-u omogući pristup podacima o zemljopisnoj, fizičkoj ili logičkoj lokaciji nadziranog sredstva za komuniciranje u slučaju postojanja telekomunikacijske aktivnosti, za razdoblje od zadnjih 12 mjeseci, vidi čl. 27. st. 2. te čl. 26. Uredbe (2008.).

77 Čl. 27. st. 2. Uredbe (2008.).

78 S ovime u vezi napominjemo da podaci koji se zadržavaju po Direktivi uključuju identifikacijske podatke, a koji se u domaćem pravnom okviru ne utvrđuju zakonom (ni ZEK-om, ni ZSOS-om), već odredbama Uredbe (2008.): ime, prezime, tj. naziv pravne osobe i adresa pretplatnika ili registriranog korisnika. Vidi čl. 110. st. 4. u vezi sa st. 1. ZEK-a te čl. 21. – 26. Uredbe (2008.), usporedi s čl. 5. Direktive. Vidi i čl. 108. st. 5. – 6. u vezi sa st. 3. ZEK-a glede obveze operatora da vode krajnji popis korisnika usluga i dostave tih podataka na zahtjev OTC-a i tijela ovlaštenih za primjenu mjera tajnog nadzora u skladu s posebnim zakonima.

Usporedna analiza Direktive i rješenja implementiranih u ZEK-u upućuje na razlike u propisanoj svrsi obveznog zadržavanja podataka jer ZEK utvrđuje bitno širu svrhu zadržavanja od Direktive, tj. propisuje zadržavanje *u svrhu istrage, otkrivanja i progona kaznenih djela u skladu s posebnim zakonom iz područja kaznenog postupka* te radi *zaštite obrane i nacionalne sigurnosti* u skladu s posebnim zakonima iz područja obrane i nacionalne sigurnosti.[79] Smatramo da je ovdje riječ o problematičnom rješenju koje proizlazi i iz opisane činjenice da je u domaćem pravnom okviru i prije transponiranja Direktive bila na snazi, a i danas je *usporedno sa ZEK-om* na snazi mjera obveznog zadržavanja podataka u elektroničkim komunikacijama prema ZSOS-u i Uredbi (2008.). Tako je rok zadržavanja podataka u ZEK-u evidentno usklađivan s rokom od godine dana, tj. 12 mjeseci predviđenim u ZSOS-u, tj. Uredbi (2008.). Što se tiče domaćih rješenja u pogledu vrsti podataka koji se moraju zadržavati, ZEK-om utvrđene odredbe u dijelu su usklađene s odgovarajućim odredbama Direktive, pa se tako njime propisuje da operatori nisu dužni zadržati podatke koje nisu obradili tijekom obavljanja (relevantnih) djelatnosti mreža i usluga[80] i da se podaci koji se odnose na nespojene pozive ne moraju zadržavati (neuspješni pokušaji poziva zadržavaju se).[81] U ZEK-u se dosljedno provodi i pravilo Direktive oko (ne)pohrane sadržaja te se, štoviše, zabranjuje zadržavanje podataka koji otkrivaju sadržaj komunikacije, što se smatra teškom povredom ZEK-a.[82] S druge strane, unatoč navedenim zakonskim odredbama koje se tiču pitanja pojedinih konkretnih vrsti podataka koji se smiju ili ne smiju zadržavati, smatramo neprimjerenim i problematičnim rješenje prema kojem se zakonom utvrđuju *kategorije* podataka koji se moraju zadržati (npr. podaci potrebni za identifikaciju izvora komunikacije i dr.), dok se za utvrđivanje *točnog popisa vrsti* podataka upućuje na Uredbu (2008.). Ovom Uredbom utvrđeni opseg (vrsta) podataka širi je, odnosno drukčiji u odnosu na Direktivu.[83] Nadalje, za

[79] Čl. 109. st. 1. ZEK-a.

[80] Čl. 109. st. 2. u vezi s čl. 109. st. 1. ZEK-a, usporedi s čl. 3. st. 1. Direktive o zadržavanju podataka.

[81] Čl. 110. st. 2. ZEK-a. Vidi i čl. 3. st. 2. Direktive o zadržavanju podataka, kao i čl. 20. st. 3. Uredbe (2008.).

[82] Čl. 110. st. 3., čl. 119. st. 1. točka 58. i čl. 119. st. 2. – 7. ZEK-a.

[83] Vidi čl. 110. st. 4. u vezi s čl. 110. st. 1. ZEK-a te čl. 20. – 26. Uredbe (2008.). Primjer je zadržavanje podataka koji se uz internetski pristup, e-poštu i internetsku telefoniju odnose i na *druge oblike podatkovne komunikacije* (čl. 21. – 25. Uredbe (2008.), usporedi s čl. 5. Direktive) te *podataka o pozivanom broju* kod *dial-up* pristupa umjesto *broja s kojeg se poziva* sukladno Direktivi, usporedi čl. 25. Uredbe (2008.) s čl. 5. st. 1. točkom e3(i) Direktive.

razliku od ranije navedenog rješenja Uredbe (2008.), prema kojem zadržani podaci za rok od 12 mjeseci moraju *biti raspoloživi* OTC-u putem propisanog tehničkog sučelja, ZEK sukladno Direktivi propisuje da se zadržavanje podataka mora provoditi tako da se podaci mogu *dostaviti* bez odgode nadležnom tijelu (u pravilu OTC-u).[84]

Provedba Direktive o zadržavanju podataka u domaći zakonodavni okvir (ZEK) donijela je dobrodošle posebne obveze radi zaštite sigurnosti zadržanih podataka i to u obliku minimalnih mjera na koje smo upozorili ranije u radu, a koje su u ZEK ugrađene ovisno o svrsi koje se njima trebaju osigurati.[85] Ove važne obveze, kako proizlazi iz propisa, odnose se samo na sustav zadržavanja koji je u domaćem pravnom okviru propisan ZEK-om. Upitno je, međutim, koliko se rješenjima koja su uvedena u ZEK doista doprinosi temeljnom cilju radi kojeg su zaštitne mjere uopće i propisane na razini Direktive. Ova primjedba odnosi se na rješenje kojim se trebala transponirati obveza Direktive, prema kojem se u domaćem pravu *morala utvrditi obveza operatora na primjenu odgovarajućih tehničkih i organizacijskih mjera kako bi zadržanim podacima moglo pristupiti samo ovlašteno osoblje.* Razlog za kritiku rješenja koje je u tom pogledu implementirano u ZEK-u temeljno je povezano s pitanjem je li u domaćem pravnom okviru ispunjena obveza utvrđivanja postupka i uvjeta koji se moraju poštovati kako bi se zadržanim podacima pristupilo u skladu sa *zahtjevima nužnosti i razmjernosti, uz poštovanje prava EU-a i međunarodnog prava te osobito Europske konvencije u skladu sa sudskom praksom Europskog suda za ljudska prava (Suda)*.[86]

Riječ je ovdje, naime, o odredbama ZEK-a koje su po našem mišljenju nedovoljno jasne i precizne[87], a kojima se utvrđuje obveza operatora da primjenjuje tehničke i ustrojstvene mjere *kako bi pristup zadržanim podacima imale samo ZEK-om propisane ovlaštene osobe, tj. tijela*. Prema našem tumačenju relevantne odredbe ZEK-a bila bi riječ o: a) operatorima/točno određenim ovlaštenim osobama operatora, ali i drugim tijelima *koja bi u posebnim okolnostima bila ovlaštena na*

---

84 Čl. 109. st. 4. u vezi s čl. 108. st. 1. ZEK-a, usporedi s čl. 8. Direktive o zadržavanju podataka.

85 Detaljno vidi u čl. 109. st. 5. ZEK-a i usporedi s člankom 7. Direktive o zadržavanju podataka.

86 Čl. 4. Direktive o zadržavanju podataka. Vidi i recital 17. Direktive.

87 "Operatori iz stavka 1. ovoga članka moraju osobito primjenjivati sljedeća načela sigurnosti zadržanih podataka: […] u slučaju kada se zadržani podaci ne upotrebljavaju u svrhe utvrđene člankom 102. ovoga Zakona, pristup zadržanim podacima mora se ograničiti isključivo na ovlaštene osobe nadležnih tijela iz članka 105. stavka 4. i članka 108. stavka 1. ovoga Zakona." Čl. 109. st. 5. točka 3. ZEK-a (vidi i čl. 109. st. 6. ZEK-a).

pristup prometnim podacima sukladno posebnim pravilima i u svrhe propisane člankom 102. ZEK-a (tako npr. i nadležni sud u slučaju spora između operatora i korisnika u vezi s iznosom dugovanja za pruženu uslugu[88]); b) *OTC-u*; c) *nadležnom tijelu policijske uprave*.

Prvo navedeno rješenje u ZEK-u uz pozivanje na propisane svrhe korištenja određenih podataka od strane operatora i drugih tijela prema članku 102. ZEK-a po našem je mišljenju pogrešno te otvara mogućnosti zloporaba podataka koji se prema navedenoj odredbi moraju zadržati ne radi npr. obračuna i naplate troškova pruženih usluga (u tu svrhu se svi ti podaci koji se moraju zadržati ni ne smiju koristiti jer dio prometnih podataka uopće nije potrebno obrađivati, a time onda ni čuvati radi obračuna pružene usluge), već isključivo u svrhu provedbe istraga, otkrivanja i kaznenog progona kaznenih djela te u svrhu zaštite obrane i nacionalne sigurnosti. Ovdje je važno imati na umu i svrhu uspostave posebnih pravila prikupljanja i obrade prometnih podataka sukladno članku 6. Direktive o e-privatnosti (koja su propisana u čl. 102. ZEK-a). Osim toga, obveze operatora na zadržavanje podataka u posebne svrhe (čl. 109. ZEK-a) ionako su utvrđene u odgovarajućoj odredbi ZEK-a *kao iznimka od primjene obveze operatora da izbriše ili anonimizira prometne podatke (koje je operator obradio i pohranio u okviru pružanja relevantnih usluga) koji se odnose na korisnike usluga, kada oni nisu više potrebni u svrhu prijenosa komunikacija*.[89]

Iz relevantne odredbe ZEK-a nadalje proizlazi da je pravo pristupa zadržanim podacima zakonodavac u najvećem broju slučajeva (s obzirom na propisanu svrhu zadržavanja) predvidio za OTC.[90] Međutim, iz rješenja koje po našem mišljenju nije dovoljno jasno i precizno, među ostalim nije razvidno je li se razmatrala tehnička pomoćna uloga ovog tijela prema Zakonu o kaznenom postupku, odnosno jesu li se sagledavale relevantne odredbe Zakona o kaznenom postupku u vezi s posebnom dokaznom radnjom prikupljanja i snimanja računalnih podataka.[91]

---

[88] Čl. 102. st. 6. ZEK-a. Usporedi s čl. 6. st. 6. Direktive o e-privatnosti te vidi C-275/06, *op. cit*. u bilj. 37, stavak 48.

[89] Čl. 102. st. 1. ZEK-a.

[90] Čl. 109. st. 5. točka 3. u vezi s čl. 108. st. 1. ZEK-a.

[91] Prema Zakonu o kaznenom postupku (ZKP), Narodne novine, br. 152/2008, 76/2009, 80/2011, 91/2012 – Odluka Ustavnog suda RH i 143/2012, OTC mora osigurati potrebnu *tehničku pomoć policiji* kod izvršavanja posebnih dokaznih radnji kojima se privremeno ograničavaju ustavna prava građana (*npr. radnja presretanja, prikupljanja i snimanja računalnih podataka*) te obavlja *tehničku koordinaciju s davateljem telekomunikacijskih usluga (oni su također dužni osigurati tehničku pomoć policiji*), vidi čl.

Konačno, zakonodavac je također ovlastio *nadležno tijelo policijske uprave* na pristup podacima korisnika usluga zadržanih, podsjećamo, u svrhu istrage, otkrivanja i kaznenog progona kaznenih djela te zaštite obrane i nacionalne sigurnosti, u *jednom posebnom slučaju*. Riječ je o novije propisanom postupku u samom ZEK-u, koji omogućuje krajnjem korisniku podnošenje podneska o navodnom zaprimanju zlonamjernih ili uznemiravajućih poziva, SMS/MMS poruka, izravno operatorima.[92] Osim toga, utvrđuje se obveza operatora na zadržavanje prometnih podataka i utvrđivanje podataka o pozivateljima/pošiljateljima (prema navodima korisnika) te njihove dostave *policijskoj upravi* (bez odgode). Detaljna analiza ovog postupka izlazi iz teme našeg rada te ćemo se ovdje ograničiti na zapažanje o tome da se prikupljanje te dostava zadržanih podataka o navodno zlonamjernim/uznemiravajućim pozivima/porukama i o korisnicima kao pozivateljima/pošiljateljima predviđa bez odluke (nadzora) suda. Dodatno, ZEK ne definira navedene vrste poziva/poruka, a jedina relevantna prekršajna odredba (uvedena 2011. g.) odnosi se (tek) na zabranu lažnog predstavljanja u javnim komunikacijskim mrežama.[93]

Možemo zaključiti da su se u ovdje analiziranoj obvezi operatora prema ZEK-u uvele posebno važne odredbe i rješenja, kojima je zakonodavac odredio ovlaštene osobe za pristup zadržanim podacima svih korisnika usluga na godinu dana, ali i svrhe njihova korištenja. Utoliko se ovakvo rješenje, držimo, ne može i ne smije razmatrati kao puko preuzimanje odgovarajuće odredbe *acquisa*, tj. Direktive. Drugim riječima, takva se rješenja moraju razmatrati u skladu

335. st. 2. ZKP-a. Posebne dokazne radnje smiju se provesti protiv osobe za koju postoje osnove sumnje da je sama počinila ili zajedno s drugim osobama sudjelovala u *relevantnom kaznenom djelu* (čl. 334.) te samo ako se istraga *ne može provesti na drugi način ili bi to bilo moguće samo uz nerazmjerne teškoće* (čl. 332. st. 1.). One se u pravilu poduzimaju na temelju pisanog obrazloženog naloga suca istrage koji se izdaje na pisani obrazloženi zahtjev državnog odvjetnika (čl. 332. st. 1.). Vidi i Pravilnik o načinu provođenja posebnih dokaznih radnji, Narodne novine, br. 102/2009.

92 Vidi čl. 109. st. 5. točku 3. u vezi s čl. 105. ZEK-a.

93 Čl. 109. st. 5. točke 3. – 4. u vezi s čl. 105. st. 3. ZEK-a, dodatno vidi čl. 120. st. 1. točku 35., čl. 120. st. 2. – 6. ZEK-a. Pretpostavljamo da je ovaj postupak pokušaj zaštite korisnika u uvjetima nedostatnog prekršajnopravnog i/ili kaznenopravnog sankcioniranja uznemiravanja putem komunikacijskih sredstava od strane nepoznatih pozivatelja (npr. neregistrirani *prepaid*, skriveni brojevi). S time u vezi vidi Vlada RH, *Prijedlog Zakona o prekršajima protiv javnog reda i mira* (1. čitanje), 4. listopada 2012., čl. 23., http://www.sabor.hr/fgs.axd?id= 21935. Vidi i Kazneni zakon, Narodne novine, br. 125/2011 i 144/2012: čl. 141. (nametljivo ponašanje, engl. *stalking*), čl. 139. (prijetnja) te Zakon o zaštiti od nasilja u obitelji, Narodne novine, br. 137/2009, 14/2010 i 60/2010: čl. 4. alineja 3.

sa *zahtjevima nužnosti i razmjernosti, uz poštovanje prava EU-a i međunarodnog prava te osobito Europske konvencije kako je u svojoj praksi tumači Sud.*

Ranije smo upozorili na obveze država da prema Direktivi osiguraju *neovisan nadzor* nad primjenom odredbi domaćih propisa kojima se provode obveze oko mjera zaštite zadržanih podataka. Držimo jasnim da nadzor ne bi smjela obavljati tijela koja istodobno pristupaju podacima, a i u samoj Direktivi predviđa se da nadzor mogu obavljati nadzorna tijela za zaštitu osobnih podataka. Međutim, ZEK propisuje da će pitanja nadzora nad primjenom načela sigurnosti zadržanih podataka biti pobliže uređena propisom koji utvrđuje obveze operatora u području nacionalne sigurnosti, *u skladu s Direktivom*.[94] Uz nejasno pozivanje na Direktivu smatramo da rješenje utvrđivanja nadzora u kontekstu Uredbe (2008.) nije prihvatljivo.[95] Smatramo neprimjerenim i rješenje da se u okviru te Uredbe utvrde i postupci prikupljanja statističkih pokazatelja o zadržanim podacima te izvješćivanje Komisije o pristupu istima.[96] Skrećemo pažnju i na po našem mišljenju neprimjereno rješenje ZEK-a kojim se (prema izmjenama i dopunama 2011. g.) provodi pravilo Direktive o e-privatnosti radi kontrole pristupa osobnim podacima, a koje smo analizirali u točki 2.1. rada. Naime, umjesto neovisnom nadzornom tijelu (npr. Agenciji za zaštitu osobnih podataka) predviđeno je da operatori dostavljaju *OTC-u* podatke o ustrojenim postupcima radi ispunjavanja obveza u vezi sa zadržavanjem podataka, broju zaprimljenih zahtjeva, pravnom temelju zahtjeva i vrsti dostavljenih podataka.[97] Po nacrtu izmjena zakona koji je bio na javnoj raspravi ove je ovlasti imala Agencija za poštu i elektroničke komunikacije[98], što je hitno izmijenjeno.[99]

Osobito imajući u vidu rezultate analize skrećemo pažnju na posebno pro-

[94] Čl. 109. st. 7. ZEK-a, usporedi s čl. 9. u vezi s čl. 7. Direktive o zadržavanju podataka.

[95] Prema Uredbi (2008.) ovlasti nadzora nad radom adresata obveza Uredbe u vezi s funkcijom tajnog nazora ima OTC u suradnji s tijelima ovlaštenima za primjenu mjera tajnog nadzora telekomunikacija, detaljnije vidi u čl. 12.

[96] Vidi čl. 10. Direktive o zadržavanju podataka.

[97] Čl. 109. st. 8. ZEK-a, usporedi s relevantnim novim stavkom 1b članka 15. Direktive o e-privatnosti.

[98] Ministarstvo mora, prometa i infrastrukture, *Javna rasprava o izmjenama i dopunama Zakona o elektroničkim komunikacijama*, http://www.mppi.hr/default.aspx?id=8981 (prijedlog novog stavka 8. članka 109.); Vlada Republike Hrvatske, *Prijedlog zakona o izmjenama i dopunama Zakona o elektroničkim komunikacijama, s Konačnim prijedlogom zakona*, 7.srpnja 2011., http://www.sabor.hr/fgs.axd?id=18448 (8. prosinca 2012.).

[99] Da je riječ o izmjeni u zadnji čas, upućuje i do danas neizmijenjena mjerodavna sankcija – sankcionira se nedostavljanje podataka *Agenciji* u skladu s čl. 109. ZEK-a (čl. 119. st. 1. točka 57. ZEK-a).

blematično rješenje s obzirom na isključenu zaštitu jamstava relevantnih prava građana. Naime, ranije u radu upozorili smo na to da se uređenje zaštite osobnih podataka primjenjuje na aktivnosti i u javnom i u privatnom sektoru.[100] Slijedom navedenoga (a uzimajući u obzir i u radu razmatrane novosti oko uređenja zaštite osobnih podataka prema pravu EU-a) po našem mišljenju sporno je i problematično rješenje kojim se predviđa opće isključenje primjene ovih propisa kod obveza operatora prema tijelima ovlaštenim za primjenu mjera tajnog nadzora.[101]

Naša osnovna analiza upućuje na potrebu temeljitog preispitivanja odredbi o zadržavanju podataka u domaćem pravnom okviru, a to se odnosi i na pojedina rješenja koja, po našem mišljenju, premašuju obveze preuzete radi usklađivanja s Direktivom o zadržavanju podataka. Pritom treba voditi računa o osiguravanju primjene načela nužnosti i razmjernosti, odnosno nužnih jamstava zaštite relevantnih temeljnih prava svih korisnika usluga – građana RH – jer se ona značajno ograničavaju mjerom obvezne preventivne pohrane brojnih podataka koji se odnose na njihovo komuniciranje kroz razdoblje od godinu dana.

3. PROVEDBA DIREKTIVE O ZADRŽAVANJU PODATAKA U EU-u

3.1. Postupci u državama članicama i pred Europskim sudom

Europska komisija nadgleda provedbu obveza država članica EU-a da transponiraju Direktivu u svoje unutarnje pravo u roku i ovlaštena je pokretati postupke protiv država za koje smatra da tu obvezu nisu ispunile (povredbeni postupak, engl. *infringement procedure*).[102] Ne ispuni li država obveze po pravu EU-a, Komisija može pokrenuti sudski postupak protiv nje pred Europskim sudom. Do kraja 2012. g. je tako u vezi s provedbom Direktive Europski sud donio presude protiv Irske, Grčke, Švedske i Austrije.[103] Osim toga, u tijeku su još povredbeni postupci protiv pojedinih država (Belgija, Češka i Rumunj-

[100] Ovo i prema Konvenciji 108 i prema ZZOP-u, detaljno vidi *supra* u bilj. 22.

[101] Vidi čl. 108. st. 4. u vezi s čl. 108. st 3. ZEK-a. Smatramo da ovdje treba poglavito imati na umu članak 141. Ustava RH prema kojem međunarodni ugovori koji su sklopljeni i potvrđeni u skladu s Ustavom i objavljeni te koji su na snazi čine dio unutarnjega pravnog poretka RH i po pravnoj su snazi *iznad zakona*.

[102] Vidi čl. 258. UFEU-a.

[103] C-202/09 *Commission* v *Ireland*, (2009) ECR, I-00203; C-211/09 *Commission* v *Hellenic Republic*, (2009) ECR, I-00204; C-185/09 *Commission* v *Kingdom of Sweden*, (2010) ECR, I-00014; C-189/09 *Commission* v *Republic of Austria*, (2010) ECR, I-00099.

ska) koje nisu implementirale Direktivu u roku.[104] Povredbeni postupci Komisije, koji mogu rezultirati i pokretanjem postupka pred Europskim sudom te izricanjem visokih novčanih kazni protiv država[105] do sada su se pokazali učinkovitim sredstvom pritiska, pa je tako velika većina država koje nisu transponirale Direktivu u roku do danas to učinila.[106] No implementacija Direktive u unutarnje pravo država članica općenito gledano nije prolazila lako. Uz izrazita negodovanja stručnjaka i aktivista za zaštitu ljudskih prava u pojedinim državama preispitivana je i valjanost domaćih odredbi[107], što je rezultiralo i

[104] European Commission, *EU law monitoring. Police co-operation and access to information infringements,* http://ec.europa.eu/dgs/home-affairs/what-is-new/eu-law-and-monitoring/infringements_by_policy_police_co-operation_and_access_to_information_en.htm (30. prosinca 2012.).

[105] Vidi članak 260. st. 3. UFEU-a.

[106] *National provisions communicated by the Member States concerning: Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC,* http://eur-lex.europa.eu (30. prosinca 2012.).

[107] *Rumunjski Ustavni sud* (*Curtea Constituţională*) 2009. g. utvrdio je neustavnost Zakona br. 298/2008 o zadržavanju podataka u elektroničkim komunikacijama: Decizia nr. 1258, din 8 octombrie 2009, dostupno pretragom (izvorni tekst i prijevod na engleski) na: http://www.legi-internet.ro/. *Češki Ustavni sud* (*Ústavní soud České republiky*) u dvije je odluke 2011. g. utvrdio neustavnost i ukinuo odredbe o zadržavanju (u zakonu o elektroničkim komunikacijama i zakonu o kaznenom postupku te uredbu o zadržavanju podataka i dostavi podataka nadležnim tijelima): Pl. ÚS 24/10 od 22.3.2011., Pl. ÚS 42/11 od 20. prosinca 2011., dostupno pretragom na: http://www. concourt.cz/. *U Bugarskoj* je 2008. g. poništena odredba uredbe o zadržavanju i dostavi podataka u svrhu nacionalne sigurnosti i kaznenih istraga, detaljnije vidi u: Nikolova, R., *Bulgaria. Supreme Administrative Court Repealed Provision Contravening Article 8 ECHR*, IRIS Legal Observations of the European Audiovisual Observatory, 3, 2009, str. 5, http://merlin.obs.coe.int/iris/2009/3/article7.en.html; *The Bulgarian Supreme Administrative Court (SAC) repeals a provision of the Data Retention in the Internet Regulation*. Statewatch News Online, 12. 2008., http://www.statewatch.org/news/2008/dec/09bulgaria-telcom-internet-decision.htm. Odluka Vrhovnog upravnog suda Bugarske br. 13627 od 11. prosinca 2008.: Върховният административен съд на Република България, Решение No. 13627, 12/11/2008, http://blog.veni.com/wp-content/uploads/2008/12/reshenievas-naredba40.pdf. Valja napomenuti i *stav ciparskog Vrhovnog suda* o neustavnosti odredbi zakona kojim se provodi Direktiva, detaljnije vidi u: Christophoros, C., *Cyprus. Provisions of the Law on Retention of Telecommunications Data Declared Unconstitutional*, IRIS Legal Observations of the European Audiovisual Observatory, 4 (rbr. članka 14), 2011, http://merlin.obs.coe.int/iris/2011/4/article14.en.html. Vrhovni sud Cipra, Odluka o provedbi Zakona 183 (I)/ 2007 (zahtjevi br. 65/2009, 78/2009, 82/2009 i 15/2010-

ukidanjem odredbi domaćih propisa o zadržavanju i dostavi podataka (ili čak cijelih propisa). Tako je npr. u Njemačkoj povodom više od 34.000 podnesenih ustavnih tužbi Savezni ustavni sud utvrdio protuustavnima te ukinuo odredbe zakona o kaznenom postupku[108] i o telekomunikacijama[109] u kojima su ugrađene pojedine odredbe Direktive. Smatrajući da se preventivnim zadržavanjem podataka koji se odnose na komunikaciju svih građana vrlo ozbiljno zadire u njihova prava, ovaj Sud zauzeo je stav da će odgovarajuće zakonske odredbe biti u skladu s ustavnopravnim jamstvom tajnosti telekomunikacija samo pod uvjetom ispunjavanja uvjeta razmjernosti, što uključuje potrebu poboljšanja zakonodavnih rješenja osobito u pogledu zaštite sigurnosti zadržanih podataka, kao i u pogledu transparentnosti i pravne zaštite. Do kraja 2012. g. u njemačkom zakonodavnom okviru još nisu usvojene nove odredbe o zadržavanju, a nacrt odredbi kojima bi se zadržavanje zamijenilo drugom mjerom prema ocjeni Europske komisije ne zadovoljava Direktivu[110], zbog čega je pokrenula postupak protiv Njemačke pred Europskim sudom[111] (ova pitanja detaljnije ćemo analizirati u četvrtom dijelu rada).

Osim navedenoga, u pojedinim državama članicama i danas su u tijeku postupci za ocjenu ustavnosti relevantnog unutarnjeg prava (npr. Mađarska[112], Slovačka[113]). Nedavno je Ustavnom sudu Republike Slovenije podnesen za-

22/2010) od 1.2.2011-*Ανωτατο Δικαστηριο Κυπρου,* Απόφαση σχετικά με την εφαρμογή του Ν. 183(Ι)/2007 για την αποκάλυψη τηλεπικοινωνιακών δεδομένων - Πολιτικές Αιτήσεις Αρ. 65/2009, 78/2009, 82/2009 και 15/2010-22/2010, dostupno pretragom na: http://www.supremecourt.gov.cy. Svim poveznicama pristupano je 30. prosinca 2012.

108 Strafprozessordnung in der Fassung der Bekanntmachung vom 7. April 1987 (BGBl. I S. 1074, 1319), die zuletzt durch Artikel 1 des Gesetzes vom 21. Dezember 2007 (BGBl. I S. 3198) geändert worden ist: § 100g st. 1., 1. rečenica u vezi s § 113a TKG-a.

109 Telekommunikationsgesetz ("TKG"), BGBl., I S. 1190., BGBl., I S. 2821: § 113a i § 113b.

110 Europa Press Releases RAPID, *Data retention: Commission takes Germany to Court requesting that fines be imposed*, IP/12/530, 31. svibnja 2012., http://europa.eu/rapid/press-release_IP-12-530_en.htm (30. prosinca 2012.).

111 C-329/12 *European Commission* v *Federal Republic of Germany*, OJ C 287, 22. rujna 2012., str. 23. Tužbom se traži i plaćanje dnevnih novčanih kazni u iznosu koji premašuje 315.000,00 eura.

112 Hungarian Civil Liberties Union – HCLU, *Constitutional Complaint Filed by HCLU Against Hungarian Telecom Data Retention Regulations*, 2. lipnja 2008., http://tasz.hu/en/data-protection/constitutional-complaint-filed-hclu-against-hungarian-telecom-data-retention (8. prosinca 2012.).

113 European Information Society Institute, *Data Retention before the Slovak Constitutio-*

htjev za ocjenu ustavnosti relevantnih odredbi zakona o elektroničkim komunikacijama, kao i za privremenu suspenziju odredbi o zadržavanju.[114] Nadalje, do kraja 2012. g. sudovi već dvije države članice postavili su pred Europskim sudom prethodna pitanja koja se odnose na valjanost Direktive u materijalnopravnom smislu. Irski Visoki sud traži među ostalim ocjenu sukladnosti Direktive s pravom na privatnost iz čl. 7. Povelje i čl. 8. Europske konvencije te s pravom na zaštitu osobnih podataka iz čl. 8. Povelje, kao i sa slobodom izražavanja prema čl. 11. Povelje i čl. 10. Europske konvencije.[115] Slično traži i austrijski Ustavni sud, a od drugih pitanja tog Suda skrećemo pažnju na tumačenje jamstva prava na zaštitu osobnih podataka prema Povelji s obzirom na čl. 8. Europske konvencije (ograničenja prava) kako ga tumači Europski sud za ljudska prava.[116]

3.2. Ocjena Direktive o zadržavanju podataka i aktualnosti

Prethodno smo upozorili na predviđeni mehanizam radi ocjene Direktive (primjena Direktive i učinak na operatore i potrošače) te razmatranja potrebe njezinih eventualnih izmjena i dopuna, osobito oko propisanog opsega i roka zadržavanja, kao i na statističke podatke koje su u vezi s time države članice dužne dostavljati Komisiji. Pomoć Komisiji u ocjeni Direktive daje i posebna

nal Court, 11. listopada 2012., http://www.eisionline.org/index.php/projekty-m/data-retention-m/49-slovak-case-on-data-retention (8. prosinca 2012.).

[114] Detaljnije u *Informacijski pooblaščenec je vložil zahtevo za oceno ustavnosti določb o obvezni hrambi podatkov o prometu elektronskih komunikacij*, http://bit.ly/XniYAt (9. travnja 2013.).

[115] Detaljnije vidi u C-293/12 *Reference for a preliminary ruling from High Court of Ireland made on 11 June 2012 - Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, The Commissioner of the Garda Síochána, Ireland and the Attorney General*, OJ C 258, 25. kolovoza 2012., str. 11. Vidi i odluku domaćeg (irskog) suda: High Court, odluka br. 2006 3785 P, *Digital Rights Ireland Ltd v Minister for Communication* & *Ors* od 5. svibnja 2010., [2010] IEHC 221.

[116] Detaljno u C-594/12 *Request for a preliminary ruling from the Verfassungsgerichtshof (Austria) lodged on 19 December 2012 – Kärntner Landesregierung and Others*, curia.europa.eu (4. ožujka 2013.). Vidi i domaću odluku suda: Verfassungsgerichtshof, Beschluss, G 47/12/11 G 59/12/10 G 62,70,71/12/11 od 28. studenoga 2012. te izvješće za medije: Verfassungsgerichtshof Österreich, *VfGH hat Bedenken gegen Vorratsdaten/Speicherung und wendet sich an EuGH*, 18. prosinca 2012., dostupno pretragom na: http://www.verfassungsgerichtshof.at (30. prosinca 2012.).

stručna skupina[117], a pri ocjeni Direktive ona je dužna razmotriti i sva zapažanja koje joj je dostavilo neovisno tijelo za zaštitu pojedinaca u vezi s obradom osobnih podataka[118] (tzv. Radna skupina članka 29, dalje u tekstu: RS29[119]).

Komisija je donijela izvješće o ocjeni Direktive 2011. godine[120] i pritom uzela u obzir i izvješće RS29 nakon ispitivanja provedbe Direktive u državama članicama.[121] Osim toga, u izvješću pridaje pažnju i stavovima europskog nadzornika zaštite osobnih podataka (dalje u tekstu: ENZOP).[122] Oba ova tijela,

---

117 *Commission Decision 2008/324/EC of 25.3.2008 setting up the "Platform on Electronic Data Retention for the Investigation, Detection and Prosecution of Serious Crime" group of experts*, OJ L 111, 23. travnja 2008., str. 11 – 14; recital 14. Direktive. Članovi su tijela vlasti nadležna za provedbu zakona, udruženja industrije elektroničkih komunikacija, predstavnik Europskoga parlamenta i nadzorna tijela za zaštitu osobnih podataka (uklj. i europski nadzornik zaštite osobnih podataka), detaljnije vidi na: http://ec.europa.eu/dgs/home-affairs/what-we-do/policies /police-cooperation/data-retention/experts-group/index_en.htm (30. prosinca 2012.)

118 Vidi čl. 14. Direktive o zadržavanju podataka.

119 Engl. *Article 29 Working Party on the Protection of Individuals with regard to the Processing of Personal Data*. RS29 neovisno je savjetodavno tijelo osnovano čl. 29. Direktive 95/46/EZ, čiji su članovi predstavnici nadzornih tijela za zaštitu osobnih podataka država članica EU-a (Agencija za zaštitu osobnih podataka RH danas ima status promatrača bez prava glasa – do pristupanja RH EU-u), europski nadzornik zaštite osobnih podataka kao predstavnik institucija i tijela EU-a te predstavnik Europske komisije. RS29 je među ostalim ovlaštena savjetovati Komisiju o svim mjerama radi zaštite prava i sloboda fizičkih osoba u vezi s obradom osobnih podataka, kao i drugim predloženim mjerama EU-a koje imaju utjecaj na ta prava i slobode. Detaljnije vidi u čl. 29. – 30. Direktive 95/46/EZ (vidi i recital 65.) te u čl. 15. st. 3. Direktive o e-privatnosti (vidi i recital 48.).

120 *Report from the Commission to the Council and the European Parliament –Evaluation report on the Data Retention Directive (Directive 2006/24/EC)*, COM(2011) 225 final, Bruxelles, 18. travnja 2011.

121 *Report 1/2010 on the second joint enforcement action: Compliance at national level of Telecom Providers and ISPs with the obligations required from national traffic data retention legislation on the legal basis of articles 6 and 9 of the e-Privacy Directive 2002/58/EC and the Data Retention Directive 2006/24/EC amending e-Privacy Directive*, 00058/10/EN, WP 172, 13. srpnja 2010. (dalje u tekstu: RS 29 – WP 172).

122 Engl. *European Data Protection Supervisor*. ENZOP je uspostavljen radi osiguravanja da institucije i tijela EU-a poštuju temeljna prava i slobode fizičkih osoba te osobito pravo na privatnost. Važnost funkcije očituje se i u obvezi Komisije da se s njime savjetuje kod usvajanja prijedloga koji se odnosi na prava i slobode u vezi s obradom osobnih podataka. Detaljnije vidi u Uredbi br. 45/2001 Europskog parlamenta i Vijeća o zaštiti osoba pri obradi osobnih podataka u institucijama i tijelima Zajednice te o slobodnome protoku takvih podataka, engl. Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protecti-

naime, davala su sukladno svojim ovlastima mišljenja i prijedloge kako u postupcima donošenja Direktive tako i nakon njezina usvajanja. Imajući u vidu zaključke Komisije o potrebi daljnjeg rada na Direktivi, spomenuta mišljenja ovih tijela iznimno su važna i evidentno se uzimaju u obzir. Budući da njihova detaljnija razrada izlazi iz okvira našeg rada, na njih u pravilu nećemo posebno upozoravati, ali ovdje skrećemo pažnju na temeljna upozorenja ovih tijela o potrebi nedvojbenog dokazivanja nužnosti mjere zadržavanja te razmjernosti s obzirom na zaštićeni interes, kao i osiguravanja snažnih mjera zaštite zadržanih podataka od bilo koje nedopuštene obrade (uključivo pristupa od strane neovlaštenih osoba).[123]

Može se reći da ocjena nužnosti mjere zadržavanja podataka s obzirom na vrlo visoku razinu zadiranja u temeljna prava i slobode građana koju takva mjera podrazumijeva predstavlja jedan od ključnih i najspornijih dijelova izvješća Komisije. Države članice nisu sve dostavile potrebne i/ili potpune podatke, a o tome u velikoj mjeri ovisi ocjena *nužnosti* uređenja mjere zadržavanja na razini prava EU-a. Taj nedostatak konkretnih i dovoljnih pokazatelja, tj. dokaza nužnosti preventivnog zadržavanja (osobito u odnosu na druga raspoloživa istražna sredstva kao što je npr. hitna zaštita pohranjenih podataka) prepoznat

on of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ L 8, 12. siječnja 2001., str. 1 – 22.

[123] U svakom slučaju, držimo da svaka podrobnija analiza izvješća Komisije i uređenja mjere zadržavanja podataka s obzirom na prava građana prema pravu EU-a zahtijeva pomno razmatranje gledišta tih tijela. Detaljnije vidi npr. u dokumentima RS29: *Opinion 4/2005 on the Proposal for a Directive of the European Parliament and of the Council on the Retention of Data Processed in Connection with the Provision of Public Electronic Communication Services and Amending Directive 2002/58/EC,* WP 113, 21. listopada 2005. (dalje u tekstu: RS29 –WP 113); *Opinion 3/2006 on the Directive 2006/24/EC of the European Parliament and of the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC,* 654/06/EN, WP 119, 25. ožujka 2006. (dalje u tekstu: RS29 – WP 119); RS 29 – WP 172, *op. cit*. u bilj. 121. Za mišljenja ENZOP-a vidi npr.: *Opinion of the European Data Protection Supervisor on the proposal for a Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC,* OJ C 298, 29. studenoga 2005., str. 1 – 12 (dalje u tekstu: ENZOP, OJ C 298, 29. studenoga 2005.); *Opinion of the European Data Protection Supervisor on the Evaluation report from the Commission to the Council and the European Parliament on the Data Retention Directive (Directive 2006/24/EC)*, 23. rujna 2011., OJ C 279, str. 1 – 10 (dalje u tekstu: ENZOP, OJ C 279, 23. rujna 2011.).

je u nizu kritika na izvješće.[124] U pogledu samog izvješćivanja država Komisija je najavila daljnji rad na poboljšanju postupka. Stoga ovdje ponovno skrećemo pažnju na po našem mišljenju nezadovoljavajuća rješenja koja su u tom smislu implementirana u domaćem pravnom okviru, kako smo već analizirali u točki 2.3. rada. S druge strane, Komisija je, bez obzira na (priznatu) manjkavost statističkih pokazatelja u izvješću, zaključila kako je zadržavanje nužno sredstvo u borbi protiv teških kaznenih djela i da je većina država zauzela stav o nužnosti ove mjere za tijela progona, zaštitu žrtava i kaznenopravne sustave. Osim toga, ona i nakon izvješća navodi da i nadalje zaprima konkretne dokaze od država koji po njoj podržavaju ocjenu o nužnosti mjere zadržavanja.[125]

Što se tiče provedbe Direktive, Komisiju zabrinjava da njome nije postignuta tražena harmonizacija domaćih propisa o zadržavanju diljem EU-a. Iako sama Direktiva dopušta poneke razlike u rješenjima (npr. oko roka i svrhe zadržavanja), ipak nalazi da su poboljšanja potrebna i u ovim aspektima. Pritom Komisija uzima u obzir i situaciju u državama članicama u kojima su pretežito ustavni sudovi ukidali odredbe o zadržavanju te njihove stavove kao i stavove posebnih neovisnih tijela (RS29 i ENZOP). Prema tome, potrebna su daljnja razmatranja načina poboljšanja sustava predviđenog u Direktivi s obzirom i na druge uključene interese (kao i načelo razmjernosti) te su nastavno na izvješće pokrenuti tzv. postupci procjena učinaka Direktive (engl. *impact assessment*) s obzirom na testove nužnosti i razmjernosti, a imajući u vidu interese unutarnje sigurnosti, unutarnjeg tržišta te jačanja poštovanja privatnosti građana i prava na zaštitu njihovih osobnih podataka. U izvješću su najavljeni daljnji koraci

[124] Vidi npr. studiju Instituta Max-Planck za strano i međunarodno kazneno pravo – Max-Planck-Institut für ausländisches und internationales Strafrecht: Albrecht, H.-J. *et al.*, *Schutzlücken durch Wegfall der Vorrats datenspeicherung? Eine Untersuchung zu Problemen der Gefahrenabwehr und Strafverfolgung bei Fehlen gespeicherter Telekommunikationsverkehrsdaten*, 2011, http://www.mpg.de/5000721/vorratsdatenspeicherung.pdf; ENZOP, OJ C 279, 23. rujna 2011., *op. cit.* u bilj. 123; European Digital Rights, *Shadow evaluation report on the Data Retention Directive*, 17. travnja 2011., http://www.edri.org/files/shadow_drd_report_110417.pdf; dopis predstavnika organizacija civilnog društva za povjerenicu Komisije za unutarnje poslove C. Malmström od 26. rujna 2011., http://www.statewatch.org/news/2011/sep/eu-mand-ret-ngo-letter-to-com.pdf (30. prosinca 2012.).

[125] *Revision of the current data retention framework (debate)*, CRE 23/10/2012-17, 23. listopada 2012. (odgovori povjerenice Komisije za unutarnje poslove C. Malmström na upite Europskog parlamenta o očekivanom prijedlogu za reviziju Direktive), dostupno pretragom na: http://www.europarl.europa.eu/ (30. prosinca 2012.).

Komisije koji uključuju i rad na razmatranju: usklađivanja roka zadržavanja[126] i mogućeg skraćivanja najduljeg roka[127] te potencijalnog utvrđivanja različitih rokova[128]; smanjenja opsega podataka[129]; načina osiguravanja nadoknade troškova za operatore (konzistentno) kao i rad na razmatranju opcija da se pojačaju standardi zaštite osobnih podataka i sigurnosti zadržanih podataka. Potonje je rezultat ocjene da države nedosljedno provode obveze vezano uz sigurnosne mjere, a riječ je o važnom pitanju i s obzirom na osobnu i osjetljivu prirodu zadržanih podataka. To uključuje i razmatranje uvođenja *privatnosti po dizajnu* kako bi se zaštita primjenjivala i kod zadržavanja i kod prijenosa podataka.[130]

Valja skrenuti pažnju i na ocjenu provedbe obveza država da odrede tijelo javne vlasti odgovorno za neovisan nadzor nad provedbom sigurnosnih mjera. Naime, kako je i predviđeno Direktivom, ovaj nadzor u većini država provode neovisna nadzorna tijelo za zaštitu osobnih podataka. Smatramo da je takva ocjena Komisije dodatni poticaj za što skoriju prilagodbu domaćeg relevantnog zakonodavnog okvira, a na što smo već upozorili u radu.[131]

Iako je u samoj Direktivi predviđeno da države članice određuju svrhu zadržavanja s obzirom na teška kaznena djela utvrđena unutarnjim pravom, uočene su znatne razlike u provedbi te svrhe, slijedom čega je Komisija najavila razmatranje potrebe za osiguravanje jačeg usklađivanja, kao i mogućnosti da se

---

126 Komisiju brine nepovoljan utjecaj različitih rokova na pravnu sigurnost i predvidljivost za operatore i građane i zbog mogućnosti multinacionalnog poslovanja operatora, a time i obrade podataka korisnika u više država EU-a.

127 U skladu s načelom razmjernosti, ali ovisno i o procjenama učinaka Direktive i naknadno dostavljenim dokazima država članica, kao i trendovima u komunikacijama i tehnologijama te kaznenim djelima i terorizmu.

128 Ovisno o vrsti podataka (npr. telefonija/internetski promet) ili teških kaznenih djela ili ovisno o kombinaciji navedenog. Iz dostavljenih podataka država članica proizlazi da nadležna tijela u gotovo 90 posto država ne traže starije podatke od šest mjeseci, dok u 70 posto i manje država ne traže podatke starije od tri mjeseca.

129 Komisija i ovdje uzima u obzir ranije stavove i tumačenja RS29, npr. o tome da se popis podataka koji se moraju zadržavati prema Direktivi mora tumačiti restriktivno te o vrstama podataka koji otkrivaju sadržaj komunikacija (destinacijske IP adrese, URL-ovi mrežnih stranica kojima su korisnici pristupali, zaglavlja elektroničkih poruka i dr.), detaljnije vidi u RS 29 – WP 172, *op. cit.* u bilj. 121, na str. 6 i 9.

130 Komisija navodi da će pritom imati na umu preporuke RS29, a najavila je i razmatranje donošenja smjernica o tehničkim i organizacijskim sigurnosnim mjerama za pristup podacima, uključujući postupke dostave podataka.

131 Vidi analizu *supra* u točkama 2.2. i 2.3. s obzirom na čl. 9. u vezi s čl. 7. Direktive te čl. 109. st. 7. ZEK-a.

to osigura.[132] Osim toga, ranije u radu upozorili smo na to da iako Direktiva ne uređuje pitanja pristupa podacima[133] države članice moraju prilikom uređenja istog osigurati *inter alia* poštovanje zahtjeva nužnosti i razmjernosti te sukladnosti osobito s Europskom konvencijom prema tumačenjima Europskog suda za ljudska prava. Komisija je utvrdila da se pravo pristupa zadržanim podacima u državama članicama daje različitim tijelima[134] i da ono nije uvijek uvjetovano odlukom neovisnog tijela, tj. suda. S obzirom na sve navedeno najavila je da će se u postupcima procjena učinaka razmatrati moguće usklađivanje pitanja pristupa podacima (npr. utvrđivanjem popisa ovlaštenih tijela, neovisnog nadzora nad zahtjevima za podacima, minimalnog standarda postupanja operatora kod odobravanja pristupa podacima). S ovim u vezi napominjemo da je jedan od glavnih problema kod ocjene provedbe Direktive ispreplетenost odredbi propisa kojima se transponiraju obveze iz Direktive s obzirom na (druge) odredbe unutarnjeg prava u kojima se uređuje zadržavanje podataka te nije jasno razlučivo kada se neka mjera jedino tiče provedbe obveza iz Direktive. Ovo je razvidno i iz analize domaćeg okvira u ovome radu.

Važno je podsjetiti na ranije u radu analizirane obveze država članica EU-a kod usvajanja mjera kojima se ograničavaju relevantna prava korisnika (i obveze operatora), kao što je mjera zadržavanja podataka, prema Direktivi o e-privatnosti. Stav je Komisije, danas, da se treba osigurati da se zadržani podaci prema Direktivi smiju koristiti samo u svrhu predviđenu Direktivom, što je u skladu s već dugo isticanim stavovima stručnjaka u području zaštite ljudskih prava te među ostalim RS29 i ENZOP-a. Ipak, izgleda da se procedura s iz-

[132] Naime, osim rješenja u kojima se izričito utvrđuje svrha zadržavanja s obzirom na teška kaznena djela kako se ona definiraju u domaćem pravnom okviru, u propisima nekih država definicija teških kaznenih djela nema, a u nekim se državama zakonom predviđa značajno šira svrha zadržavanja (i korištenja) podataka, kao npr. u svrhe istrage, otkrivanja i progona kaznenih djela općenito, kao i u svrhe zaštite nacionalne sigurnosti. Kako smo pokazali u radu, potonja situacija karakteristična je i za važeći pravni okvir u RH. Prema izvješću Komisije opisane razlike utječu na opseg i učestalost zahtjeva za podacima, a time i na troškove (za operatore) povezane s ispunjavanjem obveza iz Direktive. Osim toga, zamiječeno stanje upućuje na manjak pravne sigurnosti, odnosno predvidljivosti koja mora biti zadovoljena u svakoj zakonodavnoj mjeri kojom se ograničava pravo na privatnost.

[133] RS29 i osobito ENZOP dugo već upućuju na potrebu uređenja pristupa te korištenja zadržanih podataka.

[134] U pravilu se pristup omogućuje policiji i državnom odvjetništvu, u dijelu država i sigurnosno-obavještajnoj službi i vojsci, a u manjem broju njih također i poreznim i/ili carinskim tijelima te tijelima granične kontrole.

mjenom Direktive odugovlači. Komisija je, naime, do kraja 2012. g. najavila odgodu prijedloga za izmjenu Direktive, što je među ostalim izazvalo negativne reakcije članova Europskog parlamenta. Ona je najavila da će se izmjena Direktive *razmatrati* usporedno s *razmatranjem* izmjene Direktive o e-privatnosti glede ranije analiziranih uvjeta ograničavanja prava (utvrđivanjem mjera obveznog zadržavanja u unutarnjem pravu država članica – mimo Direktive), a radi usklađenosti rješenja sve to morat će se razmotriti i u kontekstu budućeg novog pravnog okvira zaštite osobnih podataka, koji je danas u zakonodavnom postupku.[135]

Imamo li u vidu ranije opisane posljedice ukidanja stupova EU-a u vezi s novim uređenjem zaštite osobnih podataka, kao i izmjene zakonodavnih postupaka, a osobito pojednostavljeno donošenje propisa u određenim pitanjima policijske i pravosudne suradnje[136], možemo zaključiti da se mogućnost izmjene Direktive otvara u smjeru da se u određenoj mjeri prione harmonizaciji pravila o pristupu zadržanim podacima te njihovu korištenju radi osiguravanja ujednačene zaštite prava diljem EU-a. Ipak, s obzirom na specifičnost područja i općenito interes svake države članice u području kaznenopravne zaštite može se očekivati da će taj zadatak biti posebno izazovan i da će ova tema još dulje biti aktualna. Temu ocjene Direktive i daljnjih koraka oko moguće izmjene zaključujemo kraćom analizom predlagane alternativne mjere kojom bi se potencijalno mogla ispuniti svrha Direktive uz osjetno razmjernije zadiranje, tj. uz osjetno manje zadiranje u prava i slobode (svih) građana.

4. HITNA ZAŠTITA POHRANJENIH RAČUNALNIH PODATAKA KAO ALTERNATIVA?

Uvodno smo u radu skrenuli pažnju na hitnu zaštitu pohranjenih računalnih podataka (engl. *expedited preservation of stored computer data*, skraćeno *data preservation*, popularni naziv *quick freeze*) prema Konvenciji o kibernetičkom kriminalu (dalje u tekstu: Konvencija), kao mjeru koja je još od prvih prijedloga regulacije zadržavanja na razini prava EU-a predlagana kao alternativna mjera osobito zbog znatno manje razine zadiranja u prava i slobode građana.[137] U

[135] Vidi *supra* u bilj. 120. Osim toga, vidi Council of the EU, *Note from General Secretariat of the Council to Delegations – Summary record of the meeting of the European Parliament Committee on Civil Liberties, Justice and Home Affairs (LIBE), held in Brussels on 9 and 10 July 2012*, 12557/12, 12. srpnja 2012., str. 2.

[136] Osobito vidi čl. 87. st. 2. UFEU-a.

[137] Vidi *supra* bilj. 4, na str. 8.

domaćem je pravnom okviru hitna zaštita uvedena kroz odgovarajuće odredbe Zakona o kaznenom postupku.[138] Konvencija u pogledu ove istražne mjere utvrđuje obveze država stranaka, u svrhu provedbe *određenih* kriminalističkih istraga i postupaka[139], kojima se u bitnome trebaju osigurati ovlasti nadležnih tijela da nalože hitnu zaštitu određenih računalnih podataka, uključivo prometnih podataka[140] pohranjenih uz pomoć računalnog sustava (osobito postoji li sumnja da mogu biti uništeni ili izmijenjeni).[141] Štoviše, za prometne podatke predviđena je hitna zaštita bez obzira na broj davatelja usluga uključenih u prijenos komunikacije, kao i hitno djelomično otkrivanje, tj. davanje dovoljne količine prometnih podataka nadležnom tijelu kako bi se mogli utvrditi davatelji usluga i put kojim je komunikacija prenesena.[142] Nadležna tijela trebaju imati i ovlasti naložiti dostavu podataka određenoj osobi, kao i davatelju

[138] Vidi relevantne odredbe o *dokaznoj radnji pretrage pokretnih stvari*, koja uključuje pretragu računala te s njim povezanih uređaja, drugih uređaja koji služe prikupljanju, pohranjivanju i prijenosu podataka, telefonskim, računalnim i drugim komunikacijama, kao i nositelja podataka, u vezi s čime je utvrđena obveza i *davatelja telekomunikacijskih usluga* da na zahtjev tijela koje poduzima pretragu omoguće pristup računalu, uređaju ili nositelju podataka te daju potrebne obavijesti za nesmetanu uporabu i ostvarenje ciljeva pretrage. Osim izloženoga, oni su u slučaju naloga tijela koje poduzima pretragu dužni odmah poduzeti mjere kojima se sprečava uništenje ili mijenjanje podataka (detaljnije vidi u čl. 257. ZKP-a). Osim toga, vidi odredbe o *dokaznoj radnji privremenog oduzimanja predmeta*, koja se primjenjuje i na podatke pohranjene u računalima te s njime povezanim uređajima, uređajima koji služe prikupljanju i prijenosu podataka, na nositelje podataka, *kao i na pretplatničke informacije kojima raspolaže davatelj usluga* (detaljnije vidi u čl. 263. u vezi s čl. 261. – 262. ZKP-a). U pogledu odredbe članka 257. ZKP-a skrećemo pažnju na rješenje Ustavnog suda RH osobito u vezi s pridržanim pravom ponovnog ispitivanja suglasnosti s Ustavom članka 257. ZKP-a *ex offo*. Rješenje Ustavnog suda Republike Hrvatske br. U-I-448/2009 od 19. srpnja 2012., Narodne novine, br. 91/2012., točke 210. – 213.2.

[139] Čl. 14. st. 1. Konvencije.

[140] *Računalni podaci* svako su iskazivanje činjenica, informacija ili koncepata u obliku prikladnom za obradu u računalnom sustavu, uklj. program koji je u stanju prouzročiti da računalni sustav izvrši određenu funkciju, dok su *prometni podaci* svi računalni podaci koji se odnose na komunikaciju putem računalnog sustava, koji su generirani od strane računalnog sustava koji je dio komunikacijskog lanca i koji podaci označuju podrijetlo komunikacije, odredište, put, vrijeme, datum, veličinu, trajanje ili vrstu usluge koja se koristi u mreži. Vidi čl. 1 b i d Konvencije te detaljnije u točkama 25., 28. – 31. uvodnog izvješća: Council of Europe, *Convention on Cybercrime: Explanatory Report*, http://conventions.coe.int/treaty/en/reports/html/185.htm (30. prosinca 2012.).

[141] Detaljnije vidi u čl. 16. Konvencije i točkama 158. – 164. uvodnog izvješća, *op. cit.* u bilj. 140.

[142] Detaljnije vidi u čl. 17. Konvencije i točkama 165. – 169. uvodnog izvješća, *op. cit.* u bilj. 140.

usluge[143] (pretplatnički podaci[144] koji se odnose na uslugu[145]). U tijeku rada na Konvenciji raspravljalo se o mogućnostima utvrđivanja obveze zadržavanja podataka, ali o tome nije postignut konsenzus.[146] Važnost teme pridaje se i u uvodnom izvješću uz Konvenciju s pojašnjenjem razlika između dviju mjera – hitna zaštita znači čuvanje podataka koji već postoje u pohranjenom obliku od bilo čega što može uzrokovati da se njihova sadašnja kakvoća ili stanje promijeni ili pogorša, dok obvezno zadržavanje znači čuvanje podataka koji trenutačno nastaju, za budućnost. Kako hitna zaštita služi u svrhu određenih kriminalističkih istraga, a nalog za zaštitu mora se odnositi na određene pohranjene podatke[147], ta mjera bitno se razlikuje od općeg prikupljanja podataka bez obzira na postojanje sumnje na počinjenje kaznenih djela kako bi ti podaci bili dostupni u budućnosti.[148]

Bez obzira na rana upozorenja o potrebi usmjeravanja napora za postizanjem učinkovitije provedbe mjere hitne zaštite prema Konvenciji (i jačanjem međudržavne suradnje u tom smislu) kao *razmjernije* mjere i boljeg rješenja[149] obvezno je zadržavanje na razini prava EU-a usvojeno uz stav Komisije da se hitnom zaštitom ne mogu postići ciljevi Direktive. Ipak, na ovo pitanje nastavilo se upozoravati[150] i ono je danas aktualno s obzirom na ocjenu Di-

[143] To je svako javno ili privatno tijelo koje korisnicima usluga omogućuje komuniciranje s pomoću računalnog sustava te svako drugo tijelo koje obrađuje ili pohranjuje računalne podatke za račun te komunikacijske usluge ili korisnika usluge. Vidi čl. 1c Konvencije i točke 26. – 27. uvodnog izvješća, *op. cit.* u bilj. 140.

[144] *Pretplatničke informacije* sve su informacije koje se tiču pretplatnika (osim prometnih podataka ili sadržaja komunikacije) temeljem kojih se može utvrditi: i) vrsta korištene komunikacijske usluge, poduzete tehničke mjere i razdoblje pružanja usluge; ii) identitet, poštanska ili zemljopisna adresa, broj telefona i drugi pristupni broj te informacije za slanje računa te o plaćanju, raspoložive na osnovi pretplatničkog ugovora; iii) sve druge informacije o mjestu instalacije komunikacijske opreme, raspoložive na osnovi pretplatničkog ugovora (čl. 18. st. 3. Konvencije). Detaljnije vidi u točkama 177. – 180. uvodnog izvješća, *op. cit.* u bilj. 140.

[145] Detaljnije vidi u čl. 18. Konvencije i točkama 170. – 183. uvodnog izvješća, *op. cit.* u bilj. 140.

[146] Uvodno izvješće uz Konvenciju, *op. cit.* u bilj. 140, točka 135.

[147] Nalog može biti određen na najviše 90 dana (rok čuvanja podataka do predaje ovlaštenim tijelima), a osim toga države stranke mogu predvidjeti mogućnost naknadnog obnavljanja tog naloga (čl. 16. st. 2. Konvencije).

[148] Uvodno izvješće uz Konvenciju, *op. cit.* u bilj. 140, točke 151. – 152.

[149] Vidi *supra* bilj. 4. i pripadajući tekst u radu.

[150] Vidi npr. dopis za povjerenicu Komisije C. Malmström od 22. lipnja 2010. koji supotpisuje veći broj predstavnika građana, medija, stručnjaka te industrije: http://www.statewatch.org//news/2010/jun/ngo-dataret-letter.pdf, kao i dopis predstavni-

rektive te novije momente analizirane u radu, što sve upućuje na upitnost održivosti ujednačene provedbe, diljem EU-a, sustava zadržavanja podataka kako je predviđeno Direktivom. ENZOP tako savjetuje Komisiji da, s obzirom na manje intruzivnu prirodu mjere hitne zaštite za temeljna prava, poglavito privatnost, ali i uključena procesnopravna jamstva zaštite prava osoba, ona treba napraviti daljnje istraživanje može li se tom (ili drugom) mjerom ipak *zamijeniti* zadržavanje. Ovime upotpunjuje kritiku izvješća Komisije osobito oko nedovoljno dokazane nužnosti (i razmjernosti) zadržavanja i nedovoljnog ispitivanja drugih mjera te najavu Komisije da će ona dalje razmatrati način na koji mjera hitne zaštite (ili drugi model) može *nadopuniti* (ne i zamijeniti) Direktivu.[151] No Komisija uz isticanje različitosti ovih dviju mjera i tvrdnje da većina država *smatra* da se hitnom zaštitom ne može zamijeniti zadržavanje (raspoloživost podataka)[152] kao manjak hitne zaštite navodi da ona nije propisana u svim državama strankama Konvencije i da još nema raspoloživih ocjena njezine učinkovitosti u borbi protiv kibernetičkog kriminala. Pritom uzima u obzir i "pojačani" model *quick freeze plus* u kojemu sudac može odobriti pristup i podacima koje operatori još nisu izbrisali uz nužno propisivanje, za ograničeni rok, iznimke od obveze brisanja pojedinih podataka koji su potrebni za prijenos komunikacije, ali koje operatori ne zadržavaju jer nisu potrebni za obračun (npr. podaci u vezi s pristupom internetu kod *flat-rate* tarifa). Ovdje treba imati na umu ranije prikazanu situaciju u Njemačkoj u kojoj se razmatra uvođenje hitne zaštite po modelu *quick freeze plus*, a s time u vezi i postupak pred Europskim sudom te priopćenje Komisije da usvajanjem[153] i takvog mo-

ka organizacija civilnog društva od 26. rujna 2011. g. (nakon izvješća Komisije): http://www.statewatch.org/news/2011/sep/eu-mand-ret-ngo-letter-to-com.pdf (8. prosinca 2012.), kao i RS 29-WP 113, str. 6; ENZOP, OJ C 298, 29. studenoga 2005., str. 4, a recentno osobito ENZOP, OJ C 279, 23. rujna 2011., str. 6 – 7, sve *op. cit.* u bilj. 123.

151 ENZOP, OJ C 279, 23. rujna 2011., *op. cit.* u bilj. 123.

152 Hitna zaštita primjenjuje se od nastupa sumnje u kazneno djelo, a nalog se izdaje s obzirom na određenu osobu. Komisija stoga smatra zadržavanje nužnom mjerom s obzirom na događaje nastale *prije sumnje*, radi jamstva dostupnosti *povijesnih podataka povezanih s predmetom koji se istražuje*. Kao nedostatak hitne zaštite ističe i to da ova mjera ne daje jamstvo da će biti moguće utvrditi dokaze prije izdavanja naloga, pa tako npr. ne dopušta prikupljanje podataka o kretanju žrtava, svjedoka i dr. Detaljnije vidi *supra* u bilj. 120, str. 5 (točka 3.3.).

153 Valja upozoriti i na mišljenje pravnog odjela njemačkog parlamenta o mogućoj nesukladnosti Direktive s Poveljom: Derksen, R. – Deutscher Bundestag – Wissenschaftliche Dienste, *Zur Vereinbarkeit der Richtlinie über die Vorratsspeicherung von Daten mit der Europäischen Grundrechtecharta*, Ausarbeitung WD 11-3000-18/11, 25. veljače 2011., http://www.vorratsdatenspeicherung.de/images/rechtsgutachten_

dela hitne zaštite, umjesto zadržavanja, Njemačka ne ispunjava obveze po Direktivi. Time ona daje političku poruku svima o održivosti sustava zadržavanja u pravu EU-a.[154]

S obzirom na tek pokrenute postupke pred Europskim sudom radi ocjene valjanosti Direktive i odgođeno podnošenje prijedloga izmjene ne može se očekivati da će se sporne odredbe Direktive u skorije vrijeme mijenjati, a osigurana dostupnost što veće količine podataka i u slučajevima kada ih se želi koristiti a nema dovoljno dokaza u počinjenje ili namjeru počinjenja teškog kaznenog djela, ostaje temeljnim razlogom zašto se smatra da *quick freeze* ne može zamijeniti sustav zadržavanja podataka. Posebno je važno nastaviti s daljnjim istraživanjima radi osiguravanja konkretnih dokaza o učinkovitosti obaju ovih mjera u suzbijanju i rješavanju teških kaznenih djela te istodobno poticati provedbu mjere hitne zaštite u unutarnje pravo što većeg broja država potpisnica Konvencije, a svakako svih članica EU-a.

5. ZAKLJUČNE NAPOMENE

U radu smo analizirali samo odabrane, po našem mišljenju, najvažnije okolnosti u vezi s uvođenjem i provedbom mjere obveznog preventivnog zadržavanja podataka u elektroničkim komunikacijama na razini prava EU-a i RH. Pritom je težište istraživanja bilo na utjecaju te mjere na zajamčena ljudska prava, osobito prava na poštovanje privatnog života i tajnosti dopisivanja, tj. komuniciranja te prava na zaštitu osobnih podataka.

---

grundrechtecharta.pdf. Njemačko ministarstvo pravosuđa predlaže od 2012. g. zamjenu zadržavanja mjerom hitne zaštite koja se temelji na čl. 16. Konvencije. *Quick freeze plus* daje mogućnost hitne ciljane zaštite (kod opravdanog razloga traži se zaštita podataka s obzirom na određenu osobu), a riječ je o podacima *koje operatori obrađuju u poslovne svrhe* te uspostavu obveze operatora da dostave konkretne podatke nakon što je sud izdao nalog. Posebno se radi progona *online* kaznenih djela predlaže *pohrana dinamičkih IP adresa na tjedan dana*, detaljnije vidi: Bundesministerium der Justiz, *Quick Freeze/Datensicherung*, http://www.bmj.de/DE/Buerger/digitaleWelt/QuickFreeze/quickfreeze_node.html. Hitnu zaštitu umjesto zadržavanja od 2010. g. zagovara i savezni povjerenik za zaštitu osobnih podataka i informiranje: Schaar, P., *"Quick Freeze" statt Vorratsspeicherung*, 14. lipnja 2010., dostupno pretragom na: http://www.bfdi.bund.de; Lüke, U., *Wieso der Bundesdatenschutzbeauftragte nichts mit Twitter anfangen kann, General-Anzeiger*, 20. veljače 2012., dostupno pretragom na: http://www.general-anzeiger-bonn.de/ (8. prosinca 2012.).

154 Tome u prilog ide i novija objava da većina vlada država članica dijeli njezin stav i da osobito prema novijim podacima država *zamjena* mjere zadržavanja – nije ostvariva opcija. *Op. cit.* u bilj. 125.

Smatramo da, uz najaktualniji pregled, ovo istraživanje može biti doprinos pravnoj analizi teme koja u domaćoj literaturi do danas nije značajnije obrađivana. Budući da je cilj rada ispitati odabrana ključna pitanja u zaokruženoj cjelini, zadani okvir premašili bismo dubljom razradom svakog pitanja pojedinačno. S obzirom na višeslojnost i kompleksnost analiziranog područja, očekujemo da će ovaj rad potaknuti daljnja takva istraživanja.

Rezultati naše analize relevantnog domaćeg pravnog okvira upućuju na potrebu preispitivanja pojedinih rješenja. Zbog toga, a imajući u vidu i to da se pojedinim rješenjima, donesenim radi usklađivanja hrvatskog zakonodavstva s Direktivom o zadržavanju podataka, ide dalje od navedenoga, prijedlozi koje dajemo *de lege ferenda* mogu poslužiti kako boljoj usklađenosti s *acquisom* tako i osiguranju nužnih jamstava zaštite temeljnih prava građana.

Sve okolnosti koje smo analizirali u vezi s provedbom i ocjenom Direktive u EU-u, kao i postupci radi ocjene ustavnosti i zakonitosti unutarnjeg prava u pojedinim državama i postupci koji su u tijeku pred Europskim sudom radi ocjene sukladnosti Direktive s jamstvima prava i sloboda, snažan su povod za to da se diljem EU-a razmotri jesu li kod uvođenja sustava obveznog zadržavanja podataka osigurana dovoljna jamstva prava i sloboda građana u koja se pritom zadire (uključujući zahtjeve razmjernosti i nužnosti te usklađenost s Europskom konvencijom prema tumačenjima Europskog suda za ljudska prava). Pritom uvijek treba voditi računa i o tome da je, u uvjetima brzog tehnološkog razvoja i prožetosti svakodnevnog života pojedinca korištenjem elektroničkih komunikacija, potreba uspostave odgovarajućih procesnopravnih i drugih zaštitnih mjera radi zaštite podataka u elektroničkim komunikacijama od neovlaštenog pristupa i obrade sve aktualnije pitanje u postmodernom globaliziranom društvu.

Summary

Dražen Dragičević *
Nina Gumzej **

MANDATORY DATA RETENTION AND PRIVACY

The authors analyze the regulation of the system of mandatory (preventive) retention of data in electronic communications in European Union law and the law of the Republic of Croatia. Many questions and issues of contention concerning blanket data retention regulation at EU level, especially after the adoption of the Data Retention Directive and its implementation in EU Member States, are examined in terms of sensitivity and special regulation of processing user data in electronic communications, and the severe impact of retention on guaranteed rights and freedoms of all users. The paper focuses on the impact of data retention on the right to respect for private life and communications and the right to personal data protection. The authors also analyze recent developments in the implementation of the Data Retention Directive in the EU and its evaluation by the European Commission. Procedures initiated following the implementation of this Directive in certain EU States, aimed at challenging the constitutionality and legality of relevant domestic law, point to the sensitive nature of the introduction of mandatory data retention systems on account of its interference with guaranteed rights of citizens. Furthermore, the authors also point out cases which were, until today, referred to the Court of Justice of the European Union by national courts of certain EU Member States in order to evaluate compatibility of the Directive with human rights and fundamental freedoms. The authors research and analyze solutions implemented in the domestic legal system on the subject of mandatory retention of data in electronic communications. Among other things, they call attention to the need for assessing these issues in line with the necessity and proportionality requirements, observing both European Union and international law, notably the European Convention for the Protection of Human Rights and Fundamental Freedoms and the case law of the European Court of Human Rights. Moreover, the authors emphasise the need for consistent implementation of relevant criteria in cases where guaranteed rights of citizens are interfered with, and for precise and clear legislative solutions especially with a view to preventing abuse. Finally, the authors provide a comparative overview of this measure with expedited preservation of stored data

* Dražen Dragičević, Ph. D., Professor, Faculty of Law, University of Zagreb, Trg maršala Tita 14, Zagreb

** Nina Gumzej, Ph. D., Senior Assistant, Faculty of Law, University of Zagreb, Trg maršala Tita 14, Zagreb

(data preservation, quick freeze), prescribed by the Council of Europe Convention on Cybercrime. They also provide an assessment of this measure as a potential alternative to mandatory data retention, including models developed in certain states on the basis of data preservation (quick freeze plus), taking into account recent relevant developments in the EU.

Keywords: Data Retention Directive, traffic data, confidentiality of communications, privacy, personal data protection