STRUČNI ČLANAK

UDK: 341
Primljeno: siječanj 2018.

JELENA LEVAK*, DAMIR OSTERMAN**

Zaštita, zadržavanje i razmjena podataka kojima se koriste tijela za provedbu zakonodavstva te moguća tehnička rješenja vezana uz zadržavanje podataka nakon poništenja Direktive za zadržavanje podataka presudama Suda Europske unije

Sažetak

Tijela za provedbu zakonodavstva moraju imati odgovarajući alat za zadržavanje podataka kako bi na neki način održala korak u borbi protiv terorizma i teškog kriminaliteta. Zadržavanje podataka je na razini Europske unije apsolutni osnovni element u toj borbi, no mora postojati odgovarajući balans između temeljnih prava, prava na privatnost i zaštite osobnih podataka i daljnjeg rada na sigurnosti građana. Daljnja mogućnost zadržavanja podataka od iznimne je važnosti za sigurnost građana, posebice u pogledu sprječavanja, istraga, otkrivanja i progona kaznenih djela te obrane i zaštite javne i nacionalne sigurnosti. S druge strane, zadržavanje podataka predstavlja ograničenje ljudskih prava zajamčenih Poveljom EU-a o temeljnim pravima (pravu na poštovanje privatnog života i komuniciranja, pravu na zaštitu osobnih podataka i pravu na slobodu izražavanja).

Cilj je ovog rada prikazati povijest zakonodavstva kojim se EU pokušava suočiti s problematikom borbe protiv terorizma, reformom područja zaštite podataka koja je nužno potom uslijedila kroz paket raznih zakonodavnih rješenja, presudama Suda EU u odnosu na Direktivu o zadržavanju podataka i njenim poništenjem te trenutačnim stanjem u raspravama koje su uslijedile.

* Jelena Levak, Ministarstvo unutarnjih poslova Republike Hrvatske, savjetnica za unutarnje poslove u Stalnom predstavništvu Republike Hrvatske pri Europskoj uniji, polaznica Poslijediplomskog specijalističkog studija iz kaznenopravnih znanosti na Pravnom fakultetu Sveučilišta u Zagrebu.

** Damir Osterman, Ministarstvo unutarnjih poslova, Ravnateljstvo policije, Uprava kriminalističke policije, policijski službenik, polaznik specijalističkog diplomskog stručnog studija Krizni menadžment na Veleučilištu Velika Gorica.

S tehničkog aspekta bit će prikazane mogućnosti usklađivanja, prikupljanja, obrade i pohranjivanja velikih količina podataka koji mogu poslužiti za identifikaciju osoba te kao takve moraju biti usklađene s Uredbom o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Općom uredbom o zaštiti osobnih podataka) i Direktivom o zaštiti pojedinaca u vezi s obradom osobnih podataka od strane nadležnih tijela u svrhe sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Okvirne odluke Vijeća 2008/977/PUP (tzv. Policijskom direktivom).

Kao mjere zaštite podataka u smislu navedenih propisa obradit će se šifriranje (enkripcija), anonimizacija te pseudonimizacija, uzimajući u obzir njihove prednosti i nedostatke. Obradit će se i zakonodavstvo vezano uz postupanje s podacima te koncept tehničkog rješenja koje bi imalo mogućnosti ograničavanja obrade podataka i omogućilo nadzor nad postupanjem s podacima.

Ključne riječi: *zadržavanje podataka elektroničke komunikacije, pravo na privatnost, šifriranje, anonimizacija, pseudonimizacija.*

UVOD

Počinjenjem terorističkih napada na zgrade Svjetskog trgovačkog centra u New Yorku i na Pentagon 11. rujna 2001. označen je početak "*Post 9/11*" ere, što je, između ostalog, dovelo do reakcije Vijeća sigurnosti UN-a[1]. Radi se o događaju koji je potaknuo jedinstvo zemalja i odlučnost zaustavljanja međunarodnog terorizma, pri čemu su u pogon stavljeni svi resursi, počevši od obavještajnih i vojnih resursa kao i policijskih, te diplomatskih i nakon kojeg su uslijedile opće ekonomske, socijalne, kulturne i vojne posljedice u SAD-u i drugim dijelovima svijeta.

Ti napadi promijenili su način na koji svijet gleda na sigurnost. Građani su svakim danom bili i jesu izloženi sve većem i većem broju podataka o nacionalnoj sigurnosti, međunarodnoj politici i gospodarstvu i na koji su način oni neraskidivo međusobno povezani. No i na teritoriju Europske unije (u daljnjem tekstu: EU), počevši od bombaških napada na Madrid i London (2004. i 2005.) do brojnih terorističkih napada 2015., 2016. i 2017., posljednjih se godina bilježi porast velikih terorističkih akcija.

U Zaključcima Vijeća o razvoju obnovljene strategije unutarnje sigurnosti Europske unije od 4. prosinca 2014., pod točkom 4. Temeljna prava, između ostalog navodi se i sljedeće: "Strategija unutarnje sigurnosti EU-a trebala bi doprinijeti Uniji koja štiti svoje građane i u potpunosti poštuje prava i slobode građana EU-a i onih koji imaju boravište u EU-u, borave u njemu ili ga posjećuju. Strategijom će se olakšati promicanje socijalne uključenosti i socijalne kohezije, što znači zajedno živjeti u slobodi i sigurnosti na osnovi temeljnih prava i vrijednosti EU-a, s ciljem sprečavanja pojave kriminala. Na poštovanje temeljnih prava u planiranju i provedbi politika i mjera unutarnje sigurnosti treba gledati kao na načine jamstva razmjernosti i kao alat kojim se stječe povjerenje građana i kojim ih se potiče na sudjelovanje."[2] Napomenimo kako su se samo u 2016. godini unutar Europske unije dogodila 142

[1] Vijeće sigurnosti, Resolution 1373(2001), UN Doc. S/RES/1373 (2001) od 28. rujna 2001., Vijeće sigurnosti, Report of the Policy Working Group on the United Nations and Terrorism, UN Doc. A/57/273-S/2002/875.

[2] Vijeće Europske unije 2014., Zaključci Vijeća o razvoju obnovljene strategije unutarnje sigurnosti Europske unije, Bruxelles, 4. prosinca 2014., dokument 15670/14, str. 13., dostupan na http://register.consilium.europa.

neuspjela, onemogućena ili izvršena teroristička napada, pri čemu su 1.002 osobe uhićene zbog kaznenih djela terorizma[3].

1. ZAKONODAVSTVO EUROPSKE UNIJE

1. 1. Ukratko o području suzbijanja terorizma nakon 9/11

Prije 11. rujna 2001. temom protuterorizma nije se bavio niti jedan ured ili agencija EU. Trebali su se 11. ožujka 2004. dogoditi bombaški napadi u Madridu i 7. srpnja 2005. u Londonu, kako bi se EU pokrenula i provela svoje prvo sveobuhvatno preispitivanje pitanja terorizma i to u trenutku kada je Unijom unutar rotirajućeg predsjedništva predsjedalo Ujedinjeno Kraljevstvo. Rezultat je bila Strategija EU-a za borbu protiv terorizma s ciljem globalne borbe protiv terorizma i stvaranja sigurnije Europe (2005.), koju je donijelo Vijeće. Strategija je usmjerena na četiri stupa djelovanja: prevenciju, zaštitu, progon i odgovor, a u svim je stupovima strategije prepoznata važnost suradnje s trećim zemljama i međunarodnim institucijama. Iz nje su proizašli prioriteti kao što su, između ostalog, zaštita mogućih meta i bolji zajednički odgovor na napade. Europska komisija je 15. siječnja 2014. podnijela Komunikaciju o sprječavanju radikalizacije koja dovodi do terorizma i nasilnog ekstremizma[4]. Strategija je u lipnju 2014. revidirana s obzirom na nove trendove kao što su izolirani teroristički napadi, strani borci i upotreba društvenih medija među teroristima. U prosincu 2014. Vijeće je donijelo smjernice za provedbu revidirane strategije za države članice[5].

Unatoč tome, u siječnju 2015. dogodili su se napadi na Charlie Hebdo u Parizu. Europska komisija donijela je 28. travnja 2015. Europski program sigurnosti u kojem je utvrdila glavne mjere za osiguravanje djelotvornog odgovora EU-a na terorizam i prijetnje sigurnosti u Europskoj uniji u razdoblju od 2015. do 2020[6]. Potom je u Bruxellesu u bombaškim napadima 22. ožujka 2016., od kojih se jedan dogodio nekoliko stotina metara od Komisijinog Berlaymonta, a drugi u zračnoj luci Bruxelles, poginulo najmanje 32 osobe, dok je 330 osoba lakše ili teže ranjeno, a među žrtvama je bio veliki broj različitih nacionalnosti (40)[7]. Nakon

eu/doc/srv?l=EN&f=ST%2015670%202014%20INIT, (pristup 3. studenoga 2017.).

[3] Borba EU-a protiv terorizma, dostupno na http://www.consilium.europa.eu/hr/policies/fight-against-terrorism/, (pristup 3. studenog 2017.); TESAT, EUROPEAN UNION TERRORISM SITUATION AND TREND REPORT 2017, Europol, 2017., str. 10., Izvješće u obliku PDF-a dostupno na http://www.consilium.europa.eu/hr/policies/fight-against-terrorism/, (pristup 3. studenoga 2017.).

[4] Europska komisija, KOMUNIKACIJA KOMISIJE EUROPSKOM PARLAMENTU, VIJEĆU, EUROPSKOM GOSPODARSKOM I SOCIJALNOM ODBORU I ODBORU REGIJA, Sprječavanje radikalizacije koja dovodi do terorizma i nasilnog ekstremizma: Jačanje odgovora Europske unije, COM(2013) 941 final, Bruxelles, 15. siječnja 2014., dostupno na https://ec.europa.eu/transparency/regdoc/rep/1/2013/HR/1-2013-941-HR-F1-1.Pdf (pristup 3. studenoga 2017.).

[5] Vijeće Europske unije 2014., Revidirana Strategija EU-a za borbu protiv radikalizacije i novačenja terorista, dokument broj 9956/14.

[6] Europska komisija, KOMUNIKACIJA KOMISIJE EUROPSKOM PARLAMENTU, VIJEĆU, EUROPSKOM GOSPODARSKOM I SOCIJALNOM ODBORU I ODBORU REGIJA Europski program sigurnosti, COM(2015) 185 final, Strasbourg, 28. travnja 2015., dostupno na http://eur-lex.europa.eu/legal-content/HR/ALL/?uri=CELEX:52015DC0185, (pristup 2. studenoga 2017.).

[7] Deutsche Welle, *Brussels bombing aftermath - live updates*, dostupno na http://www.dw.com/en/brussels-bombing-aftermath-live-updates/a-19135323, (pristup 2. studenoga 2017.).

navedenih napada pokrenut je Europski program sigurnosti za borbu protiv terorizma i stvaranje uvjeta za uspostavu učinkovite i istinske sigurnosne Unije[8], u čijem se uvodu navodi: "Europska unija uspostavljena je kako bi se njezinim građanima osiguralo područje slobode, sigurnosti i pravde bez unutarnjih granica. Europljani moraju biti sigurni da su, kamo god se kretali unutar Europe, njihove slobode i sigurnost dobro zaštićene, čime se u potpunosti poštuju vrijednosti Unije, uključujući vladavinu prava i temeljna prava. U tom pogledu osnivačkim je ugovorima predviđena potreba za osiguranjem visoke razine sigurnosti, između ostalog i zahvaljujući preventivnim mjerama te koordinaciji i suradnji policijskih, sudskih i drugih nadležnih tijela[9]. Zato EU i njene države članice trebaju izići iz okvira suradnje u cilju zaštite unutarnje nacionalne sigurnosti i započeti djelovati vođene idejom zaštite kolektivne sigurnosti Unije u cjelini". Ukratko, potrebno je prijeći s koncepta suradnje radi zaštite nacionalne unutarnje sigurnosti na ideju zaštite kolektivne sigurnosti Unije kao cjeline, s posebnim naglaskom na bolju razmjenu podataka. U području protuterorističkog djelovanja i radikalizacije Europski program sigurnosti osmišljen je u cilju provedbe ciljanih operativnih mjera povezanih s posebnim rizicima i neposrednog jačanja kolektivne sposobnosti EU-a za suzbijanje terorizma. U okviru prioriteta borbe protiv terorizma Europski program sigurnosti usredotočen je na prijetnje od povrataka stranih terorističkih boraca, prevenciju radikalizacije te sankcioniranje terorista i njihovih pristalica. Istaknuta je važnost blokiranja pristupa terorista financiranju, oružju i eksplozivima, poboljšanja zaštite građana i ključne infrastrukture te rješavanja vanjske dimenzije u borbi protiv terorizma izvan granica EU-a. Naglašena je i važnost bolje razmjene informacija radi djelotvornog praćenja osoba uključenih u terorističke aktivnosti. Ta ključna područja interesa ojačana su Akcijskim planom o vatrenom oružju i eksplozivima donesenim u prosincu 2015.[10], o jačanju borbe protiv financiranja terorizma donesenim u veljači 2016.[11] te Komunikacijom o jačim i pametnijim informacijskim sustavima za granice i sigurnost donesenom 6. travnja 2016[12].

---

[8] Europska komisija, KOMUNIKACIJA KOMISIJE EUROPSKOM PARLAMENTU, EUROPSKOM VIJEĆU I VIJEĆU o provedbi Europskog programa sigurnosti za borbu protiv terorizma i stvaranje uvjeta za uspostavu učinkovite i istinske sigurnosne unije; ANNEX 1, PRILOG KOMUNIKACIJI KOMISIJE EUROPSKOM PARLAMENTU, EUROPSKOM VIJEĆU I VIJEĆU o provedbi Europskog programa sigurnosti za borbu protiv terorizma i stvaranje uvjeta za uspostavu učinkovite i istinske sigurnosne Unije, COM/2016/230 final, Bruxelles, 20. travnja 2016., dostupno na http://eur-lex.europa.eu/legal-content/HR/TXT/?uri=CELEX:52016DC0230, (pristup 2. studenoga 2017.)

[9] Članak 67. stavak 3. UFEU-a.

[10] Europska komisija, KOMUNIKACIJA KOMISIJE EUROPSKOM PARLAMENTU I VIJEĆU, Provedba Europskog programa sigurnosti: Akcijski plan EU-a za borbu protiv nezakonite trgovine vatrenim oružjem i eksplozivima te njihove uporabe, COM/2015/0624 final, Bruxelles, 2. Prosinca 2015., dostupno na http://eur-lex.europa.eu/legal-content/HR/TXT/?uri=CELEX:52015DC0624#footnote3, (pristup 2. studenoga 2017.).

[11] Europska komisija, KOMUNIKACIJA KOMISIJE EUROPSKOM PARLAMENTU I VIJEĆU o Akcijskom planu za jačanje borbe protiv financiranja terorizma, COM/2016/050 final, Bruxelles, 2. veljače 2016., dostupno na http://eur-lex.europa.eu/resource.html?uri=cellar:e6e0de37-ca7c-11e5-a4b5-01aa75ed71a1.0023.02/DOC_1&format=PDF, (pristup 2. studenoga 2017.).

[12] Europska komisija, KOMUNIKACIJA KOMISIJE EUROPSKOM PARLAMENTU I VIJEĆU Jači i pametniji informacijski sustavi za granice i sigurnost, COM(2016) 205 final, Bruxelles, 6. travnja 2016., dostupno na http://eur-lex.europa.eu/legal-content/HR/TXT/?uri=CELEX:52016DC0205, (pristup 2. studenoga 2017.).

1.2. Zaštita podataka

S novom, često na internetu temeljenom tehnologijom, koja igra sve važniju ulogu u organiziranju i sprječavanju takvih akata masovnog nasilja, počele su se pojavljivati napetosti između potreba sigurnosti i čvrsto ukorijenjenih prava EU na zaštitu podataka i privatnost. To se posebice očitovalo 2013. godine kada je "zviždač" Edward Snowden razotkrio SAD i UK prakse masovnog nadzora što je dovelo do propitivanja postojećeg kompromisa između osiguravanja sigurnosti i zaštite prava na privatnost kroz veliko i neselektivno prikupljanje i analizu podataka pod pokroviteljstvom nacionalne sigurnosti i borbe protiv terorizma[13].

Posljedično, Europska komisija je 2015. predložila sveobuhvatnu reformu EU zakonodavstva za zaštitu podataka iz 1995. kako bi ojačala *online* privatnost i potakla europsko digitalno gospodarstvo.

Nakon četverogodišnjeg pregovaranja EU je 2016. usvojila paket koji se sastojao od Opće uredbe o zaštiti osobnih podataka (EU 679/2016)[14] i Direktive (EU 2016/680) o zaštiti pojedinaca u vezi s obradom osobnih podataka od strane nadležnih tijela u svrhe sprječavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija i o slobodnom kretanju takvih podataka (tzv. Policijska direktiva)[15]. Obje uključuju jačanje prava na djelotvorni pravni lijek i omogućavaju ulaganje pritužbi te osiguravaju snažan nadzor nezavisnih nacionalnih tijela za zaštitu podataka, koja mogu primati pritužbe i dodijeliti naknadu podnositeljima zahtjeva.

Nadalje, usvojena je i Direktiva o uporabi podataka iz evidencije podataka o putnicima u svrhu sprječavanja, otkrivanja, istrage i progona kaznenih djela terorizma i teških kaznenih djela (PNR direktiva)[16], s ciljem reguliranja prijenosa podataka iz PNR-a o putnicima na međunarodnim letovima od zračnih prijevoznika državama članicama, kao i obradu tih podataka koju obavljaju nadležna tijela. Kao treće veliko područje nametnulo se pitanje nevaljanosti Direktive o zadržavanju podataka[17] (od 2014.), no o tome nešto više kasnije u tekstu.

---

[13] Zrinka Salaj, Međunarodnopravne implikacije masovnog nadzora elektroničkih komunikacija u kontekstu ljudskih prava, s posebnim osvrtom na sigurnosno-obavještajni sustav u Republici Hrvatskoj, ZPR 6 (1) 2017; str. 15.-40.

[14] Službeni list Europske unije, L 119/1, 4. svibnja 2016., UREDBA (EU) 2016/679 EUROPSKOG PARLAMENTA I VIJEĆA od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka).

[15] Službeni list Europske unije, L 119/89, 4. svibnja 2016., DIREKTIVA (EU) 2016/680 EUROPSKOG PARLAMENTA I VIJEĆA od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka od strane nadležnih tijela u svrhe sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Okvirne odluke Vijeća 2008/977/PUP.

[16] Službeni list Europske unije, L 119/132, 4. svibnja 2016., DIREKTIVA (EU) 2016/681 EUROPSKOG PARLAMENTA I VIJEĆA od 27. travnja 2016. o uporabi podataka iz evidencije podataka o putnicima (PNR) u svrhu sprečavanja, otkrivanja, istrage i kaznenog progona kaznenih djela terorizma i teških kaznenih djela.

[17] Službeni list Europske unije, L 105/54, 13. travnja 2004., DIREKTIVA 2006/24/EZ EUROPSKOG PARLAMENTA I VIJEĆA od 15. ožujka 2006. o zadržavanju podataka dobivenih ili obrađenih u vezi s pružanjem javno dostupnih elektroničkih komunikacijskih usluga ili javnih komunikacijskih mreža i o izmjeni Direktive 2002/58/EZ.

1.3. Obrada osobnih podataka

Pored prikupljanja i zaštite osobnih podataka, teroristički napadi usmjerili su pozornost i na zadržavanje podataka elektroničke komunikacije od strane pružatelja telekomunikacijskih usluga kao alata za zaštitu nacionalne sigurnosti i rješavanje kaznenih djela. U nastavku dajemo pregled zakonodavnih akata EU-a u području zaštite podataka.

Europski parlament i Vijeće donijeli su 24. listopada 1995. godine direktivu 95/46/EZ o zaštiti pojedinaca u pogledu obrade osobnih podataka i o slobodnom kretanju takvih podataka[18]. Ova direktiva poznata je kao Direktiva o zaštiti osobnih podataka. Primjenjuje se na podatke obrađene automatiziranim sredstvima (npr. računalna baza podataka kupaca) i podatke koji su sadržani ili namjeravaju biti sadržani u neautomatiziranom sustavu pohrane podataka. Direktiva je usmjerena na zaštitu prava i sloboda osoba na području obrađivanja osobnih podataka kada je obrada podataka dopuštena te posebno njihovo pravo na privatnost.

Potom je 1997. godine usvojena Direktiva 97/66/EZ o obradi osobnih podataka i zaštiti privatnosti u području telekomunikacija, koja je potom, jer se morala prilagoditi razvoju na tržištima i u tehnologijama elektroničkih komunikacijskih usluga kako bi mogla pružiti jednaku razinu zaštite osobnih podataka i privatnosti korisnicima javno dostupnih elektroničkih komunikacijskih usluga, neovisno o tehnologijama koje se koriste, 12. srpnja 2002. godine zamijenjena Direktivom 2002/58/EZ o obradi osobnih podataka i zaštiti privatnosti u području elektroničkih komunikacija[19]. Ona čini dio paketa odredbi o telekomunikacijama i poznata je kao Direktiva o privatnosti i elektroničkim komunikacijama. Prije svega odnosi se na obradu osobnih podataka prilikom isporuke komunikacijske usluge. U svom uvodnom dijelu navodi kako se uvode nove napredne digitalne tehnologije u javne komunikacijske mreže, što dovodi do posebnih zahtjeva u vezi sa zaštitom osobnih podataka i privatnosti korisnika. Razvoj informacijskog društva karakterizira uvođenje novih elektroničkih komunikacijskih usluga, a pristup digitalnim pokretnim mrežama postao je dostupan i prihvatljiv široj javnosti. Te digitalne mreže imaju ogromne kapacitete i mogućnosti obrade osobnih podataka. Uspješan prekogranični razvoj tih usluga djelomice ovisi o povjerenju korisnika da njihova privatnost neće biti ugrožena. Internet mijenja tradicionalne tržišne strukture pružajući zajedničku globalnu infrastrukturu za dostavu širokog raspona elektroničkih komunikacijskih usluga. Javno dostupne elektroničke komunikacijske usluge preko interneta otvaraju korisnicima nove mogućnosti, ali i nove opasnosti za njihove osobne podatke i privatnost. Davatelji usluga elektroničke komunikacijske usluge moraju štititi sigurnost svojih usluga sljedećim mjerama: osiguravanjem osobnih podataka, a pristup tim podacima dozvoliti samo ovlaštenim osobama; zaštitom osobnih podataka kako se ne bi uništili, izgubili ili bili promijenjeni; osiguravanjem provedbe sigurnosne politike na području obrade osobnih podataka.

U Direktivi je navedeno da države članice moraju, kao i prema svojim nacionalnim zakonima, osigurati tajnost komunikacije koja se odvija preko javne elektroničke komunikacijske mreže. Slušanje, snimanje i skladištenje komunikacijskih podataka mora biti izričito zabranjeno osobama koje nisu korisnici bez pristanka navedenih korisnika. Direktiva određu-

[18] Dostupno na http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:31995L0046, (pristup 29. studenoga 2017.).

[19] Dostupno na http://eur-lex.europa.eu/legal-content/HR/ALL/?uri=CELEX:32002L0058 (pristup 29. studenoga 2017.).

je da se podaci o prometu i lokacijski podaci moraju brisati ili učiniti anonimnima kada više nisu potrebni za održavanje komunikacije ili za obračun, osim ako je pretplatnik dao svoj pristanak za drugu uporabu. Između ostalog u članku 15. stavku 1. navodi se da: "Države članice mogu donijeti zakonske mjere kojima će ograničiti opseg prava i obveza…, kada takvo ograničenje predstavlja nužnu, prikladnu i razmjernu mjeru unutar demokratskog društva s ciljem zaštite javne i nacionalne sigurnosti (odnosno državne sigurnosti), obrane te s ciljem sprečavanja, istrage, otkrivanja i progona kaznenih djela odnosno neovlaštene uporabe elektroničkog komunikacijskog sustava iz članka 13. stavka 1. Direktive 95/46/EZ. S tim u vezi, države članice mogu, između ostalog, donijeti zakonske mjere kojima se omogućuje zadržavanje podataka tijekom ograničenog razdoblja opravdane razlozima određenim u ovom stavku. Sve mjere iz ovog stavka moraju biti u skladu s općim načelima prava Zajednice, uključujući ona iz članka 6. stavka 1. i 2. Ugovora o Europskoj uniji."

2. DIREKTIVA O ZADRŽAVANJU PODATAKA I PRESUDE SUDA EUROPSKE UNIJE

Godine 2006. usvojena je Direktiva 2006/24/EZ o zadržavanju podataka dobivenih ili obrađenih u vezi s pružanjem javno dostupnih elektroničkih komunikacijskih usluga ili javnih komunikacijskih mreža (Direktiva o zadržavanju podataka) s glavnim ciljem usklađivanja zakonodavnih rješenja država članica koje se odnose na obveze zadržavanja određenih podataka koje skupljaju ili obrađuju pružatelji javno dostupnih elektroničkih komunikacijskih usluga ili javnih komunikacijskih mreža. Na taj način ona je osiguravala dostupnost tih podataka u svrhu sprječavanja, istrage, otkrivanja i progona teških kaznenih djela, poput kaznenih djela povezanih s organiziranim kriminalom i terorizmom. Direktiva je predviđala da navedeni pružatelji moraju zadržati podatke o prometu i lokaciji kao i s tim povezane podatke nužne za identificiranje pretplatnika ili korisnika. Nasuprot tome, nije dopuštala zadržavanje sadržaja komunikacije i informacija kojima se pristupa. Ključne odredbe Direktive bile su: obveza zadržavanja podataka (čl. 3.) i pristup podacima (čl. 4.) te kategorije podataka koji se zadržavaju, trajanje zadržavanja i područje primjene.

Direktiva je potom bila podvrgnuta čitavom nizu tužbi pred Sudom EU. Sud EU je presudom u spojenim predmetima *Digital Rights Ireland* i *Seitlinger* i dr.[20] 2014. godine direktivu proglasio nevaljanom jer omogućava široko i osobito teško miješanje u temeljna prava na poštovanje privatnog života i na zaštitu osobnih podataka, a koje nije ograničeno samo na ono što je strogo nužno. Takvim poništenjem nastalo je stanje pravne nesigurnosti posebice vezano uz pravne statuse nacionalnih zakonodavstava kojima se ta Direktiva prenosila i samoj dostupnosti takvih podataka tijelima za provedbu zakona i njihovoj uporabi kao dokaza u kaznenom postupku. Iako je Sud priznao da je Direktiva ostvarila legitiman cilj u borbi protiv teškog kriminala i zaštite nacionalne sigurnosti, Sud je utvrdio kako u dovoljnoj

[20] Službeni list Europske unije, C 175/6, 10. lipnja 2014., Presuda Suda (Veliko vijeće) od 8. travnja 2014. (zahtjev za prethodnu odluku koji su uputili High Court of Ireland, Verfassungsgerichtshof – Irska, Austrija) – Digital Rights Ireland Ltd (C-293/12), Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl i dr. (C-594/12) protiv 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 (Spojeni predmeti C-293/12 i C-594/12).

mjeri nisu osigurane zaštitne mjere kojima bi se zaštitila privatnost i osigurala dovoljna razina zaštite podataka. Osnovni zaključci Suda bili su da zadržavanje podataka mora biti ograničeno (ne može obuhvaćati sve osobe, sva sredstva komunikacije i sav podatkovni promet bez ikakvog razlikovanja); pristup i uporaba podataka moraju biti ograničeni (pristup mogu imati samo nadležna tijela i koristiti ih samo u one svrhe zbog kojih su podaci i prikupljani); trajanje zadržavanja mora biti razmjerno; podaci se obavezno moraju zadržavati na području Unije i potrebna je zaštita zadržanih podataka od rizika zlouporabe[21].

Potom je švedski *Tele2* pokrenuo novi sudski postupak koji je rezultirao presudom Suda EU u dvama spojenim predmetima C-203/15 i C-698/15 (*Tele2 i Watson*)[22]. U presudi Sud navodi da se nacionalnim zakonodavstvom, kojim se određuje obveza općenitog i neselektivnog zadržavanja svih podataka o prometu i lokaciji prekoračuju granice onoga što je potrebno te pojasnio kriterije i uvjete koje trebaju ispuniti nacionalni mehanizmi zadržavanja podataka država članica. Tako je Sud naveo kako države članice mogu odstupiti od povjerljivosti komunikacija i s njima povezanih podataka o prometu kada je to vremenski ograničeno, nužno, prikladno i strogo razmjerno. Sud je također naveo kako ciljana nacionalna mjera za zadržavanje podataka može biti osigurana samo u svrhu borbe protiv teškog kriminala. Zadržavanje podataka ne može biti opće i neselektivno zadržavanje svih podataka o prometu i lokaciji svih pretplatnika i registriranih korisnika koji se odnose na sva sredstva elektroničke komunikacije. (Što potvrđuje i Mišljenje Suda u predmetu vezanom uz EU-Kanada PNR sporazum[23]. Dakle, nizom presuda (C-362/14, C-582/14, C-203/15 i C-698/15, C-293/12, itd.) Sud EU-a istaknuo je proaktivni stav o osiguranju zaštite podataka.

---

[21] Sud Europske unije, PRIOPĆENJE ZA MEDIJE br. 54/14, Luxembourg, 8. travnja 2014., Presuda u spojenim predmetima C-293/12 i C-594/12 Digital Rights Ireland i Seitlinger i dr., dostupno na https://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054hr.pdf, (pristup 29. studenoga 2017.).

[22] Presuda Suda (Veliko vijeće) od 21. prosinca 2016., Tele2 Sverige AB i Secretary of State for the Home Department protiv Post-och telestyrelsen i dr. (zahtjevi za prethodnu odluku koje su uputili Kammarrätten i Stockholm i Court of Appeal (England & Wales) (Civil Division), "Zahtjev za prethodnu odluku – Elektroničke komunikacije – Obrada osobnih podataka – Povjerljivost elektroničkih komunikacija – Zaštita – Direktiva 2002/58/EZ – Članci 5., 6. i 9. i članak 15. stavak 1. – Povelja Europske unije o temeljnim pravima – Članci 7., 8. i 11. i članak 52. stavak 1. – Nacionalno zakonodavstvo – Pružatelji elektroničkih komunikacijskih usluga – Obveza koja se odnosi na opće i neselektivno zadržavanje podataka o prometu i podataka o lokaciji – Nacionalna tijela – Pristup podacima – Nepostojanje prethodnog nadzora suda ili nadzora neovisnog upravnog tijela – Usklađenost s pravom Unije.", (spojeni predmeti C-203/15 i C-698/15), dostupno na http://eur-lex.europa.eu/legal-content/HR/TXT/?uri=CELEX%3A62015CJ0203#t-ECR_62015CJ0203_HR_01-E0001, (pristup 1. studenoga 2017.).

[23] Mišljenje Suda (Veliko vijeće) od 26. srpnja 2017. – Europski parlament (mišljenje 1/15), (Mišljenje na temelju članka 218. stavka 11. UFEU-a – Prijedlog sporazuma između Kanade i Europske unije – Prijenos podataka iz popisa imena zrakoplovnih putnika iz Unije u Kanadu – Odgovarajuće pravne osnove – Članak 16. stavak 2., članak 82. stavak 1. drugi podstavak točka (d) i članak 87. stavak 2. točka (a) UFEU-a – Usklađenost sa člancima 7. i 8. te člankom 52. stavkom 1. Povelje Europske unije o temeljnim pravima), dostupno na http://curia.europa.eu/juris/document/document.jsf?docid=194498&mode=req&pageIndex=1&dir=&occ=first&part=1&text=&doclang=HR&cid=73014#1, (pristup 4. rujna 2017.).

3. POSLJEDICE PONIŠTENJA DIREKTIVE O ZADRŽAVANJU PODATAKA U DRŽAVAMA ČLANICAMA EUROPSKE UNIJE

Države članice Europske unije koje takvom odlukom Suda EU-a više nisu obvezane na temelju specifičnog pravnog instrumenta Unije uvesti ili održavati nacionalni režim zadržavanja podataka različito su pristupile presudi. Neke su zadržale postojeće stanje, dok su druge krenule s izmjenama, zamjenama ili stavljanjem izvan snage zakonodavstva kojima se Direktiva prenijela ili njegovim poništenjem od strane nacionalnih sudova. Iako se radi o promjenjivoj situaciji, u ovom trenu možemo dati sljedeću podjelu: novi nacionalni propisi: Belgija, Bugarska, Njemačka, Rumunjska, Slovačka, Italija i UK; bez nacionalnih propisa: Austrija, Nizozemska i Slovenija; zadržale postojeće nacionalne propise: Cipar, Češka, Danska, Estonija, Finska, Francuska, Grčka, Hrvatska, Irska, Latvija, Litva, Luksemburg, Mađarska, Malta, Poljska, Portugal, Španjolska i Švedska (Švedska je 9. listopada 2017. izašla s izvješćem svoje posebne komisije u kojem se nalaze novi prijedlozi na koji način uskladiti švedske nacionalne propise kako bi bili kompatibilni sa zakonodavstvom EU-a.).

Europska komisija je zauzela stav da neko vrijeme neće izlaziti s novim zakonodavstvom na ovu temu već da će radije proučiti nacionalna zakonodavstva država članica i kako ona provode zadržavanje podataka. Na razini Vijeća EU-a na ovu temu osnovana je, unutar radne skupine za razmjenu informacija i zaštitu osobnih podataka (DAPIX), posebna formacija Prijatelja Predsjedništva (*Friends of Presidency Data Retention*), tijekom čijih su rasprava države članice istaknule negativne posljedice navedene presude na učinkovitost kaznenih istraga na nacionalnoj razini te se ukazalo na potrebu za zajedničkim pristupom na razini EU-a s ciljem utvrđivanja pravnih i praktičnih rješenja izazova koji proizlaze iz sudske prakse Suda EU-a.

Glavni problem je nedostatak usklađenog pristupa zadržavanju podataka na razini EU od kada je donesena presuda u predmetu (*Digital Rights Ireland*), s obzirom na to da je poništenjem direktive nestala zakonska obveza zadržavanja podataka. Sud je u svojoj presudi naveo da ciljana nacionalna mjera za zadržavanje podataka može biti osigurana samo u svrhu borbe protiv teškog kriminala. U presudi *Digital Rights Ireland* Sud navodi da "veza između zadržanih podataka i ostvarene svrhe i/ili dodatnih zaštitnih mjera u vezi s pohranom i pristupom može zadržavanje podataka učiniti legitimnim". Stroži uvjet nametnula je Tele2 presuda "opće zadržavanje podataka je samo po sebi nezakonito bez obzira na zaštitne mjere koje se provode. Zadržavanje podataka ne smije postati pravilo".

Najnoviji smjer predstavlja tumačenje presuda *Data Protection Function Europola* i Koordinatora EU-a za borbu protiv terorizma. Prema njihovu tumačenju presude, podrazumijeva se da općenito zadržavanje podataka pod zakonodavstvom EU-a nije moguće, ali da je moguće ograničeno zadržavanje podataka. Opće zadržavanje podataka jasno je zabranjeno prema pravu EU-a, što znači da je masovno pohranjivanje podataka bez jasne svrhe zabranjeno. Međutim, u presudi *Tele2* navodi se da postoji mogućnost ograničenog zadržavanja podataka (*restricted data retention*) odnosno ograničenog pohranjivanja podataka. Ograničavajući podatke, pohranjivali bi se samo podaci koji su relevantni za tijela za provođenje zakonodavstva, a koja unaprijed ne znaju koji su to podaci. Važno je odrediti koje su kategorije podataka potrebne ili koje su potencijalno važne jer će nakon definiranja tih kategorija podataka zadržavanje podataka biti moguće. Dodatni smjer predstavlja zadržavanje podataka u odnosu na sve osobe, no uz dodatne zaštitne mehanizme, zadržavanje podataka ograničeno na podatke potencijalno relevantne za tijela za provedbu zakonodavstva i ciljani pristup za-

držanim podacima. Uvijek postoji i mogućnost izrade nove Direktive, što bi administrativno moglo biti vrlo zahtjevno, uz vjerojatne dugotrajne rasprave na razini radnih skupina stručnjaka, pa potom i na političkoj razini suzakonodavaca. Naposljetku, vrata su dodatno ostala odškrinuta i po pitanju novog prijedloga Uredbe o e-Privatnosti[24].

Na razini EU-a nastavljaju se daljnje rasprave, no u očekivanju rješenja države članice su itekako svjesne da velika većina njih ima na snazi propise koji su u proturječju sa sudskom praksom Suda EU-a, neke uopće nemaju nacionalno zakonodavstvo, dok su neke donijele nove propise koje trenutačno ponovno propituju njihovi nacionalni sudovi.

4. ZADRŽAVANJE PODATAKA U REPUBLICI HRVATSKOJ

Izmjenama i dopunama Zakona o kaznenom postupku 2002. godine[25] u članku 177. stavku 2. prvi put se pojavljuje točno definirana ovlast kojom redarstvene snage mogu od pravne osobe pružatelja telekomunikacijskih usluga zatražiti provjeru istovjetnosti telekomunikacijskih adresa koje su u određenom razdoblju uspostavile vezu dok se prije ovih izmjena pristup zadržanim podacima provodio na temelju istog članka Zakona o kaznenom postupku iz 1997. godine, odnosno na dio koji se odnosi na druge potrebne mjere i radnje.

Kompleksniji pristup zadržavanju podataka i nadzoru telekomunikacija tijekom godina ostvaruje se donošenjem niza zakonskih propisa kojima se uređuje ovo pitanje i donosi sveobuhvatan pravni i tehnički okvir kojim su definirani ciljevi i svrha korištenja ove ovlasti te definirani instrumenti nadzora nad korištenjem ovlasti u svrhu zaštite od zlouporabe pristupa zadržanim podacima:

- Zakon o kaznenom postupku (NN 110/97., 58/02., 152/08., 76/09., 80/11., 121/11., 91/12., 143/12., 56/13., 145/13. i 152/14.),
- Zakon o policijskim poslovima i ovlastima (NN 76/09. i 92/14.),
- Zakon o sigurnosno-obavještajnom sustavu Republike Hrvatske (NN 79/06. i 105/06.),

---

[24] Prijedlog UREDBE EUROPSKOG PARLAMENTA I VIJEĆA o poštovanju privatnog života i zaštiti osobnih podataka u elektroničkim komunikacijama te stavljanju izvan snage Direktive 2002/58/EZ (Uredba o privatnosti i elektroničkim komunikacijama), COM(2017) 10 final, Bruxelles, 10. siječnja 2017., dostupno na: http://eur-lex.europa.eu/legal-content/HR/TXT/?uri=CELEX%3A52017PC0010, (pristup 29. studenoga 2017.).

[25] Zakon o kaznenom postupku u članku 177. stavku 2. navodi: "Radi ispunjenja zadataka iz stavka 1. ovoga članka redarstvene vlasti mogu tražiti potrebne obavijesti od građana, primijeniti poligrafsko testiranje, analiziranje glasa, obaviti potreban pregled prijevoznih sredstava, osoba i prtljage, za prijeko potrebno vrijeme nadzirati i ograničiti kretanje određenih osoba na određenom prostoru (promatranje, pratnja, blokada, racija, zasjeda, klopka, nadzor prijenosa stvari i dr.), poduzeti potrebne mjere u svezi s utvrđivanjem istovjetnosti osoba i predmeta, raspisati potragu za osobom i stvarima, u nazočnosti odgovorne osobe obaviti pregled određenih objekata i prostorija državnih tijela, pravnih osoba te drugih poslovnih prostora i ostvariti uvid u određenu njihovu dokumentaciju i podatke, prikupljati obavijesti uz prikrivanje svrhe prikupljanja ili s prikrivanjem svojstva policijskog službenika, putem tajnog izvjestitelja, od pravne osobe koja pruža telekomunikacijske usluge zatražiti provjeru istovjetnosti telekomunikacijskih adresa koje su u određenom razdoblju uspostavile vezu, te poduzeti druge potrebne mjere i radnje. O činjenicama i okolnostima koje su utvrđene prilikom poduzimanja pojedinih radnji, a mogu biti od interesa za kazneni postupak, sastavit će se službena zabilješka."

- Zakon o elektroničkim komunikacijama (NN 73/08., 90/11., 133/12., 80/13. i 71/14.),
- Uredba o obvezama iz područja nacionalne sigurnosti Republike Hrvatske za pravne i fizičke osobe u telekomunikacijama (NN 83/03., 64/08. i 76/13.),
- Zakon o telekomunikacijama (NN 122/03.),
- Zakon o sigurnosno-obavještajnom sustavu Republike Hrvatske (NN 79/06. i 105/06.),
- Zakon o obrani (NN 73/13.),
- Pravilnik o vojnopolicijskim poslovima i provedbi ovlasti ovlaštenih službenih osoba Vojne policije (NN 44/2014.).

Do značajne se promjene u zadržavanju i pristupu zadržanim podacima dolazi donošenjem Zakona o sigurnosno-obavještajnom sustavu Republike Hrvatske koji ne samo da u članku 18. definira Operativno-tehnički centar za nadzor telekomunikacija (u daljnjem tekstu OTC) kao tehničko tijelo koje obavlja aktivaciju i upravlja mjerom tajnog nadzora telekomunikacijskih usluga, djelatnosti i prometa te kao koordinacijsko tijelo između operatora javnih telekomunikacija i tijela za provođenje zakona[26] - već i kao tijelo koje je u potpunosti uredilo međusobne odnose te obveze operatora kroz niz tehničkih pravila koja su usklađena s preporukama Europskog instituta za telekomunikacijske norme (ETSI)[27] u pogledu pohrane, pristupa, prijenosa i sigurnosti podataka te nacionalnim zakonskim propisima i interesima nacionalne sigurnosti.

Ovakav ujednačeni pristup operatorima doveo je do uklanjanja svih dvojba oko svrhe i načina zadržavanja podataka, vrsta podataka koje se zadržavaju, formata zapisa podataka, vremenskog roka za zadržavanje podataka, procesa brisanja podataka, postupka osiguranja podataka i infrastrukture te evidentiranja pristupa podacima.

4.1. Pristup zadržanim podacima

Obveza zadržavanja podataka za operatore u Zakonu o elektroničkim komunikacijama propisana je člankom 109. u kojemu se osim obveze zadržavanja podataka na 12 mjeseci od dana obavljene komunikacije, propisuje i svrha, sigurnost, kvaliteta i zaštita podataka te dodatne obveze operatora. Članak 110.[28] istog Zakona propisuje koje podatke su operatori

---

[26] Zakon o sigurnosno-obavještajnom sustavu u članku 18. navodi: "Radi obavljanja aktivacije i upravljanja mjerom tajnog nadzora telekomunikacijskih usluga, djelatnosti i prometa te ostvarivanja operativno-tehničke koordinacije između pravnih i fizičkih osoba koje raspolažu javnom telekomunikacijskom mrežom i pružaju javne telekomunikacijske usluge i usluge pristupa u Republici Hrvatskoj i tijela koja su ovlaštena za primjenu mjera tajnog nadzora telekomunikacija sukladno s ovim Zakonom i Zakonom o kaznenom postupku, osniva se Operativno-tehnički centar za nadzor telekomunikacija (u daljnjem tekstu: OTC).".

[27] "*European Telecommunications Standards Institute*" - http://www.etsi.org/

[28] Zakon o elektroničkim komunikacijama, članak 110. propisuje sljedeće vrste zadržanih podataka:
"(1) Obveza zadržavanja podataka iz članka 109. ovoga Zakona obuhvaća sljedeće vrste podataka:
– podatke potrebne za praćenje i utvrđivanje izvora komunikacije,
– podatke potrebne za utvrđivanje odredišta komunikacije,
– podatke potrebne za utvrđivanje nadnevka, vremena i trajanja komunikacije,

dužni zadržavati te izričito zabranjuje zadržavanje podataka koji otkrivaju sadržaj komunikacije. U tome smislu zadržanim podacima o ostvarenom telekomunikacijskom prometu smatraju se svi podaci potrebni za ostvarivanje te komunikacije te podaci o vremenu i lokaciji komunikacije. Policijski službenici Ministarstva unutarnjih poslova, pristup zadržanim podacima ostvaruju na temelju dvaju zakonskih propisa i to članka 339.a Zakona o kaznenom postupku[29] i članka 68. Zakona o policijskim poslovima i ovlastima.[30]

Slijedeći inicijalne tehničke postavke stvorene od strane OTC-a, pravila pristupa podacima te okvire utvrđene zakonskim propisima, Ministarstvo unutarnjih poslova stvorilo je informacijsko-komunikacijski okvir za upravljanje zahtjevima za odobrenje pristupa zadržanim podacima putem OTC-a pod nazivom TIRM (*Telecommunication Information Request Management*) čime je napravljen veliki iskorak u pogledu zaštite podataka, kontrole pristupa, transparentnosti postupanja te ubrzanja procedura kroz ovakav u potpunosti informatizirani proces po vertikalnoj i horizontalnoj liniji ustroja. Cijeli proces informatizacije proveden je od najniže razine ustrojstvenih jedinica, odnosno policijskih postaja do Uprave kriminalističke policije u Ravnateljstvu policije.

Poštujući hijerarhiju ustroja Ravnateljstva policije te odredbe članka 68. Zakona o policijskim poslovima i ovlastima, svi zahtjevi za odobrenje pristupa zadržanim podacima

– podatke potrebne za utvrđivanje vrste komunikacije,
– podatke potrebne za utvrđivanje korisničke komunikacijske opreme ili opreme koja se smatra korisničkom komunikacijskom opremom,
– podatke potrebne za utvrđivanje lokacije pokretne komunikacijske opreme.
(2) Zadržani podaci iz stavka 1. ovoga članka obuhvaćaju i podatke koji se odnose na neuspješne pozive, pri čemu nema obveze zadržavanja podataka o pozivima koji uopće nisu bili uspostavljeni.
(3) Zabranjeno je zadržavanje podataka koji otkrivaju sadržaj komunikacije.
(4) Podrobnije odrednice o pojedinim vrstama zadržanih podataka iz stavka 1. ovoga članka utvrđuju se posebnim propisom koji uređuje obveze iz područja nacionalne sigurnosti za pravne i fizičke osobe u elektroničkim komunikacijama, u skladu s mjerodavnom direktivom Europske unije o zadržavanju podataka.".

[29] U stavku 1. i 2. članka 339.a Zakona o kaznenom postupku navodi se zakonski temelj i mogućnosti traženja pristupa zadržanim podacima: "(1) Ako postoji sumnja da je registrirani vlasnik ili korisnik telekomunikacijskog sredstva počinio kazneno djelo iz članka 334. ovog Zakona ili neko drugo kazneno djelo za koje je propisana kazna zatvora teža od pet godina policija može, na temelju naloga suca istrage, a radi prikupljanja dokaza, putem Operativno-tehničkog centra za nadzor telekomunikacija od operatora javnih komunikacijskih usluga zatražiti provjeru istovjetnosti, trajanja i učestalosti komunikacije s određenim elektroničkim komunikacijskim adresama, utvrđivanje položaja komunikacijskog uređaja, kao i utvrđivanje mjesta na kojima se nalaze osobe koje uspostavljaju elektroničku komunikaciju, te identifikacijske oznake uređaja.
(2) Za registriranog vlasnika ili korisnika telekomunikacijskog sredstva koji je povezan s osobom za koju postoji sumnja da je počinila kazneno djelo iz članka 334. ovog Zakona ili neko drugo kazneno djelo za koje je propisana kazna zatvora teža od pet godina policija može, na temelju naloga suca istrage, putem Operativno-tehničkog centra za nadzor telekomunikacija zatražiti od operatora javnih komunikacijskih usluga provjeru iz stavka 1. ovog članka.".

[30] U stavku 1. i 2. članka 68. Zakona o policijskim poslovima i ovlastima naveden se zakonski temelj i mogućnosti traženja pristupa zadržanim podacima: "(1) Radi sprječavanja i otkrivanja kaznenih djela za koja se progoni po službenoj dužnosti i njihovih počinitelja, sprječavanja opasnosti i nasilja, traganja za osobama i predmetima, policija može od davatelja komunikacijskih usluga zatražiti provjeru istovjetnosti, trajanja i učestalosti komunikacije s određenim elektroničkim komunikacijskim adresama.
(2) Zahtjev iz stavka 1. ovoga članka može obuhvaćati i utvrđivanje položaja komunikacijskog uređaja, kao i utvrđivanje mjesta na kojima se nalaze osobe koje uspostavljaju elektroničku komunikaciju te identifikacijske oznake uređaja."

prije odobrenja od strane načelnika Uprave kriminalističke policije, načelnika Policijskog nacionalnog ureda za suzbijanje korupcije i organiziranog kriminaliteta ili načelnika policijskih uprava, provjereni su i odobreni odnosno odbijeni od strane rukovoditelja ustrojstvenih jedinica kojima su nadređeni.

Sve navedeno omogućuje u potpunosti transparentan i provjerljiv okvir za pristup zadržanim podacima jer se svaka akcija u sustavu bilježi bez mogućnosti brisanja ili uređivanja jednom popunjenog i poslanog zahtjeva za odobrenje pristupa zadržanim podacima.

Svi zahtjevi za odobrenje pristupa zadržanim podacima moraju biti detaljno obrazloženi na način koji kroz to obrazloženje daje jasnu sliku nadređenom rukovoditelju o razlozima obavljanja ove vrste provjere, a ne neke manje invazivne, podatke o prethodno poduzetim radnjama koje su dovele do ove vrste provjere, očekivane rezultate te druge relevantne podatke koji potvrđuju opravdanost zahtjeva za odobrenje pristupa zadržanim podacima.

Praksa je pokazala kako je uvođenje ovakvog informacijsko-komunikacijskog okvira za pristup zadržanim podacima u smislu zaštite podataka i prava građana omogućilo jednostavniju i sigurniju razmjenu podataka, učinkovitiji nadzor nad zakonitosti provedbe ovlasti te sustavno i kvalitetno statističko praćenje pristupa.

S druge strane, prednosti ovakvog pristupa za policiju su:

- jedinstvena točka pristupa,
- pristup svim operatorima s jednog mjesta,
- jedinstvena baza znanja,
- kontrolni elementi već ugrađeni u sustav,
- intuitivno kretanje kroz sučelje,
- pohrana podataka na centralnom mjestu,
- kolaborativnost kroz sustav,
- sustavi izvješćivanja na svim rukovodećim razinama,
- brzina reakcije za pomoć žrtvama kaznenih djela,
- učinkovitije i brže mogućnosti kod traganja za nestalim osobama.

4.2. Važnost zadržavanja podataka

U današnjem digitalnom društvu koje u potpunosti prihvaća nove informacijsko-komunikacijske tehnologije, zadržavanje podataka pod jasno definiranim uvjetima od ključnog je značaja za istraživanje svih vrsta kaznenih djela s ciljem povećanja javne sigurnosti, otkrivanja počinitelja te u slučajevima traganja za osobama koje su žrtve kaznenih djela, vlastite nepromišljenosti ili drugih okolnosti. U takvom društvu, digitalni tragovi ostavljaju se svakodnevno bez obzira na to koristi li se tehnologija ili samim pojavljivanjem na javnim prostorima koji su pokriveni takvim tehnologijama.

Digitalni tragovi evidentiraju se, pohranjuju i obrađuju prilikom svake financijske transakcije (banke, bankomati, *online* plaćanja i sl.), na nadzornim kamerama, sustavima ulaza i izlaza (zgrade, autoceste, granični prijelazi i dr.), programima vjernosti raznih trgovačkih lanaca ili *online* trgovina. O ostavljenim digitalnim tragovima na ovim sustavima, čak i kada

je to dragovoljno, malotko postavlja pitanja poput: "Kako se koriste moji podaci? Kome su dostupni? Postoji li ikakva zaštita? Kada se podaci brišu?". Kod ovakvih programa uglavnom postoji zainteresiranost samo za ostvarivanje bilo kakve koristi ili zadovoljavanja neke od potreba.

S druge strane, zadržavanjem podataka o komunikaciji korisnik ne ostvaruje nikakvu korist do trenutka dok ne postane žrtva nekog kaznenog djela i jedini trag koji može dovesti do počinitelja ili u početku usmjeriti istragu u pravom smjeru nalazi se upravo u nekom od podataka navedenih u članku 109. Zakona o elektroničkim komunikacijama.

Zadržani podaci o komunikaciji i pristup tim podacima, policiji i pravosudnim vlastima, služe kao alat kojim mogu učinkovito i u razumnom roku pomoći žrtvama kaznenih djela, tragati za nestalim osobama, rekonstruirati tijek događaja koji su doveli do kaznenog djela ili pak mogli utjecati na nestanak osobe ili počinjenje kaznenog djela; utvrditi druge sudionike osim počinitelja i žrtve poput organizatora ili pomagača te mogućih svjedoka.

Žrtva često ne mora biti neka osoba pojedinac jer u težim kaznenim djelima korupcije, prijevara u gospodarskom poslovanju, organiziranom kriminalitetu ili terorizmu, žrtve su i same države odnosno svi njezini građani koji kroza svoj rad i plaćanja poreza sudjeluju u životu države i njenom gospodarskom i političkom rastu i razvoju. Ovo je još jedan dodatni argument koji ide u prilog činjenici da je javna sigurnost stup nacionalne sigurnosti, dok je zadržavanje podataka i pristup zadržanim podacima, policiji neprocjenjiv alat koji joj omogućuje održavati percepciju i stvarno stanje javne sigurnosti na visokoj razini povećanom otkrivačkom djelatnošću i djelotvornim traganjem za osobama.

4.3. Razdoblje zadržavanja podataka

Kao što je već navedeno, propisano razdoblje zadržavanja podataka i njihove dostupnosti u Republici Hrvatskoj jest 12 mjeseci od dana ostvarene komunikacije, dok na području država članica EU-a ovo razdoblje nije ujednačeno i kreće se od općenite zabrane zadržavanja u kojoj ne postoje povijesni podaci do razdoblja od posljednje 3 godine.

Republika Hrvatska procijenila je kako je razdoblje od 12 mjeseci dovoljno kako bi se provodila učinkovita kriminalistička istraživanja i prevencija kaznenih djela i terorizma s ciljem očuvanja javne sigurnosti svih građana.

Iako postoje zadržani podaci za razdoblje od 12 mjeseci, policija bi ovakvoj ovlasti prikupljanja podataka za razdoblja duža od 6 mjeseci trebala pristupati samo iznimno i pod jasno obrazloženim okolnostima. Razlog zadržavanja podataka do 12 mjeseci leži u činjenici da sva teška kaznena djela, posebno u sferi korupcije i gospodarskog kriminaliteta imaju svoje duže, kontinuirano vrijeme počinjenja, a saznanje o postojanju kaznenog djela ne dolazi u trenutku početka počinjenja već tek kada se vide posljedice istoga. Vrijeme saznanja za neko kazneno djelo, počinjeno ili mu je počinjenje u tijeku, predstavlja važan čimbenik za donošenje odluke o tome za koje vremensko razdoblje zatražiti pristup zadržanim podacima i kojim točno podacima.

5. PRISTUP ZADRŽANIM PODACIMA I ZAŠTITA PODATAKA

Kada se prihvati činjenica da je zadržavanje podataka neophodno za sigurnost svih građana, tada prestaje rasprava o zadržavanju podataka i može se povesti rasprava isključivo o pristupu zadržanim podacima te njihovim načinima zaštite.

Kao što je naprijed navedeno, Zakon o sigurnosno-obavještajnom sustavu Republike Hrvatske već je propisao uspostavu posebnog tehničkog tijela, OTC-a, koje je između ostalih poslova zaduženo i za komunikaciju s pružateljima usluga u telekomunikacijama te osiguravanje pristupa zadržanim podacima.

Zakonodavac je policiji, naime, Zakonom o policijskim poslovima i ovlastima te Zakonom o kaznenom postupku precizno propisao uvjete i načine pristupa zadržanim podacima što je rezultiralo uspostavom kvalitetnog i provjerljivog cjelovitog okvira za pristup podacima koji pruža sve elemente zaštite podataka i omogućuje sprječavanje bilo kakvog pokušaja zlouporabe ove ovlasti.

5.1. Pseudonimizacija, enkripcija, odobrenje pravosudnog ili drugog nadzornog tijela

Kako bi pristup zadržanim podacima bio u skladu s presudama Suda EU-a (pod pretpostavkom pronalaska zakonodavnog okvira za zadržavanje podataka na razini EU-a) potrebno je detaljno razmotriti sve dodatne mjere zaštite koje postoje ili ne postoje te ih unaprijediti ili nadograditi sukladno s utvrđenim stanjem. To su ponajprije mjere poput pseudonimizacije, enkripcije, dodatnog odobrenja pravosudnog ili drugog neovisnog nadzornog tijela.

U preporukama Vijeća Europe CM/Rec(2016)5 o slobodama na internetu naglašeno je da: "države ne zabranjuju, zakonski ili u praksi, anonimnost, pseudonimizaciju, povjerljivost privatne komunikacije ili uporabu metoda enkripcije dodajući da **uplitanje u anonimnost i povjerljivost komunikacija treba ispunjavati zahtjeve legalnosti, legitimnosti i proporcionalnosti** opisanih u članku 8. Europske povelje o ljudskim pravima[31]."

Ovi elementi zaštite ključni su i u segmentu sprječavanja zlouporabe zadržanih podataka, pa je u tome pogledu Ministarstvo unutarnjih poslova napravilo dodatne napore te stvorilo informacijsko-komunikacijski okvir za upravljanje odobrenjima i zahtjevima za pristup zadržanim podacima nazvan TIRM. Ovakav pristup pokazao se kao kvalitetan i siguran te je osim ubrzanja operativnog pristupa zadržanim podacima u hitnim situacijama traganja za osobama, omogućio i dodatne financijske uštede i to prije svega u pogledu troškova uredskog materijala, dostave i radnih sati te izuzetnu zaštitu od mogućih zlouporaba na svim razinama.

[31] Vijeće Europe, Odbor ministara (2016), Preporuka CM/Rec (2016)5 Odbora ministara državama članicama o slobodi interneta, 13. travnja 2016., točka 4.1.7.

5.1.1. Anonimizacija

Potvrda da je, u ovome trenutku, anonimizacija u potpunosti siguran način zaštite osobnih podataka može se pronaći i u činjenici da Opća uredba o zaštiti osobnih podataka u Uvodnoj izjavi 26[32] navodi da se ne primjenjuje na osobne podatke koji su učinjeni anonimnima na način da se identitet pojedinca više ne može utvrditi. Iako je ovo naizgled idealan način zaštite osobnih podataka, isto tako ovaj način zaštite zadržanih podataka trenutačno ne može biti prihvatljiv tijelima za provedbu zakona jer bi to u potpunosti poništilo pozitivne učinke koje za javnu sigurnost omogućuje zadržavanje podataka. No iako se ovo čini savršenom zaštitom osobnih podataka, razvoj tehnologije i novih tehnika ovu metodu u budućnosti može učiniti ranjivijom, odnosno moguće je da će u određenom trenutku u vremenu biti moguće identificirati anonimizirane podatke. U tome trenutku ova tehnika zaštite podataka mogla bi postati prihvatljiva tijelima za provedbu zakona. Logično je stoga zaključiti da bi vlasnici baza sa osobnim podacima povremeno trebali revidirati stanje anonimiziranih podataka te potvrditi da je mjera još uvijek dostatna za zaštitu podataka.

5.1.2. Pseudonimizacija

Opća uredba o zaštiti osobnih podataka[33] u članku 4. stavku 1. točki 5. definira pseudonimizaciju na sljedeći način:

"(5) "pseudonimizacija" znači obrada osobnih podataka na način da se osobni podaci više ne mogu pripisati određenom ispitaniku bez uporabe dodatnih informacija, pod uvjetom da se takve dodatne informacije drže odvojeno te da podliježu tehničkim i organizacijskim mjerama kako bi se osiguralo da se osobni podaci ne mogu pripisati pojedincu čiji je identitet utvrđen ili se može utvrditi;"

Pseudonimizirani podaci i dalje predstavljaju osobne podatke, ali pseudonimizacija je propisana kao dodatna mjera zaštite osobnih podataka kako oni ne bi bili u punom opsegu dostupni širem krugu pojedinaca. Kao takva, pseudonimizacija smanjuje rizik od identifikacije

---

[32] Službeni list Europske unije, L 119/1, 4. svibnja 2016., UREDBA (EU) 2016/679 EUROPSKOG PARLAMENTA I VIJEĆA od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka), (26) Načela zaštite podataka trebala bi se primjenjivati na sve informacije koje se odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi. Osobne podatke koji su pseudonimizirani, a koji bi se mogli pripisati nekom pojedincu uporabom dodatnih informacija trebalo bi smatrati informacijama o pojedincu čiji se identitet može utvrditi. Kako bi se odredilo može li se identitet pojedinca utvrditi, trebalo bi uzeti u obzir sva sredstva, poput primjerice selekcije, koja voditelj obrade ili bilo koja druga osoba mogu po svemu sudeći upotrijebiti u svrhu izravnog ili neizravnog utvrđivanja identiteta pojedinca. Kako bi se utvrdilo je li po svemu sudeći izgledno da se upotrebljavaju sredstva za utvrđivanje identiteta pojedinca, trebalo bi uzeti u obzir sve objektivne čimbenike, kao što su troškovi i vrijeme potrebno za utvrđivanje identiteta, uzimajući u obzir i tehnologiju dostupnu u vrijeme obrade i tehnološki razvoj. Načela zaštite podataka stoga se ne bi trebala primjenjivati na anonimne informacije, odnosno informacije koje se ne odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi ili na osobne podatke koji su učinjeni anonimnima na način da se identitet ispitanika ne može ili više ne može utvrditi. Ova se Uredba stoga ne odnosi na obradu takvih anonimnih informacija, među ostalim za statističke ili istraživačke svrhe.

[33] Ibid., članak 4. stavak 1. točka 5.

pojedinaca tijekom same obrade podataka. Također, uzimajući u obzir današnja informacijska dostignuća, pseudonimizacija ne predstavlja veliki trošak kod uvođenja, a za razliku od anonimizacije i dalje omogućuje nesmetani rad tijela za provedbu zakona uz već spomenute zakonske i tehničke okvire pristupa podacima.

5.1.3. Enkripcija

Uvodna izjava Direktive (EU) 2016/680 (tzv. Policijska direktiva) navodi sljedeće:

"(60) Kako bi se očuvala sigurnost i spriječila obrada kojom se krši ova Direktiva, voditelj obrade ili izvršitelj obrade trebao bi procijeniti rizike povezane s obradom te bi trebao provesti mjere za njihovo ublažavanje, kao što je enkripcija. Takvim bi se mjerama trebala osigurati odgovarajuća razina zaštite, uključujući povjerljivost, te uzeti u obzir najnovija dostignuća i troškovi provedbe u odnosu na rizik i vrstu osobnih podataka koji se trebaju zaštititi. Prilikom procjene rizika za sigurnost podataka u obzir bi trebalo uzeti rizike koje predstavlja obrada podataka poput slučajnog ili nezakonitog uništenja, gubitka, izmjene ili neovlaštenog otkrivanja osobnih podataka ili pristupa osobnim podacima koji su preneseni, pohranjeni ili na drugi način obrađivani, a što osobito može dovesti do fizičke, materijalne ili nematerijalne štete. Voditelj obrade i izvršitelj obrade trebali bi osigurati da obradu osobnih podataka ne provode neovlaštene osobe."

Uz činjenicu da enkripcija postaje sve jednostavnija za implementaciju i uporabu te da ima sve manje negativan utjecaj na iskustvo korisnika u situacijama kada je ista uključena, ovakva mjera sigurnosti sigurno je dobar način zaštite osobnih podataka. Tijekom uvođenja enkripcije, potrebno je voditi brigu o tome da se postupak enkripcije provodi ne samo na strani pohrane podataka već i tijekom prijenosa podataka kao i o tome da kriptirane baze budu pretražive uz aplikativni pristup koji također u svom dizajnu ima sustave za enkripciju.

5.1.4. Odobrenje pravosudnog ili drugog nadzornog tijela

Kako je cijeli postupak pristupa zadržanim podacima u sustavu Ministarstva unutarnjih poslova uspostavljen uporabom informacijsko-komunikacijskih tehnologija, uvođenje dodatnog stupnja odobrenja od strane pravosudnog ili drugog neovisnog nadzornog tijela ne bi trebalo postavljati dodane prepreke niti dodatno produljivati vrijeme potrebno za dohvat zadržanih podataka. To je potrebno postići omogućavanjem pristupa takvom tijelu prema informacijsko-komunikacijskom rješenju koje bi istome, kao i policijskim službenicima, bilo dostupno u svako doba dana i noći.

Propisivanjem točno određene procedure, kategorije podataka, svrhe pristupanja i drugih sigurnosnih elemenata moguće je uvesti ovakvo tijelo u postupak koji ima izravne veze s provođenjem kriminalističkih istraživanja i spašavanja života, ali kako je već i navedeno, samo uz prihvaćanje postojećih informacijsko-komunikacijskih rješenja i bez utjecaja na tijek i tempo provođenja istraživanja.

5.2. Sustav za dostavu i upravljanje digitalnim dokazima

Inovativan i siguran način za dostavu digitalnih dokaza, uz pripremljen zakonodavni okvir, treba imati i mogućnost praćenja od trenutka početnog stvaranja digitalnog dokaza do prezentacije istih na sudu kako bi u potpunosti mogli biti prihvatljivi kao valjani dokazi. Uspostavom ovakvog načina dostave kroz sustav za dostavu i upravljanje digitalnim dokazima moguće je provesti sljedeće funkcionalnosti unutar jednog informacijsko-komunikacijskog rješenja:

- kontrolu nad prikupljanjem dokaza,
- zaštitu dokaza od faze prikupljanja do faze izvođenja na sudu,
- očuvanje povijesnih podataka o dokazu,
- kontroliranu dopunu sustava mišljenjem sudskog vještaka,
- sprječavanje izmjene dokaza,
- rješavanje problema nedostatka nadzora nad dokazima.

Kod postojanja ove vrste sustava za dostavu i upravljanje digitalnim dokazima, vlasnik podatka trebao bi u svakom trenutku biti u mogućnosti obaviti nadzor nad korištenjem dostavljenih podataka te postaviti mehanizme za enkripciju ili pseudonimizaciju u određenom trenutku u vremenu kod pribavljanja dokaza. Također, vlasniku podatka, korištenjem ove vrste okvira za upravljanje digitalnim dokazima, ostaje mogućnost nadzora nad izvozom dostavljenih podataka iz ovakvog sustava.

6. ZAKLJUČAK

Tijela za provedbu zakonodavstva moraju imati odgovarajući alat za zadržavanje podataka kako bi na neki način održala korak u borbi protiv terorizma i teškog kriminaliteta. Zadržavanje podataka je na razini Unije apsolutni osnovni element u toj borbi, no mora postojati odgovarajuća ravnoteža između temeljnih prava, prava na privatnost i zaštite osobnih podataka te daljnjeg rada na sigurnosti građana. Zadržavanje osobnih podataka ne smije prelaziti ono što je neophodno za svrhe za koje se obrađuju osobni podaci (ograničenje pohrane, članak 5. stavak 1. točka e) Opće uredbe o zaštiti podataka). Nastojanja država članica u jačanju obavještajnih službi i tijela za provedbu zakonodavstva poslužila su kao svojevrsni okidač da ih različite međunarodne organizacije pozovu na suzdržavanje, uz pozivanje svih stranaka na poštovanje relevantnih međunarodnih i europskih pravnih standarda. Iz predavanja UN-ovog specijalnog izvjestitelja za pravo na privatnost, profesora Josepha A. Cannatacia, koje je održao 30. siječnja 2017. na St. Julianu na Malti,[34] razvidno je kako je on predložio pomak u pristupu koji se odnosi na promjenu pristupa s "privatnost vs. sigurnost" na "privatnost i sigurnost", pri čemu se oba prava smatraju "kao prava koja omogućavaju, a ne završavaju sama po sebi"[35]. Također je napomenuo kako su mnoge zemlje požurile kroz nacionalne par-

[34] Autorica je pribivala neformalnoj raspravi.

[35] United Nations (UN), Human Rights Council, Cannataci, J. (2016), Report of the Special Rapporteur on the right to privacy, A/HRC/31/64, 8. ožujka 2016., str.9., točka 23., dostupno na https://documents-dds-ny.un.org/doc/UNDOC/GEN/G16/262/26/PDF/G1626226.pdf?OpenElement, (pristup 3. prosinca 2017.).

lamente uvesti zakonodavstva koja ugrožavaju privatnost[36].

Daljnja mogućnost zadržavanja podataka od iznimne je važnosti za sigurnost građana, posebice u pogledu sprječavanja, istraga, otkrivanja i progona kaznenih djela te obrane i zaštite javne i nacionalne sigurnosti. S druge strane, zadržavanje podataka predstavlja ograničenje ljudskih prava zajamčenih Poveljom EU-a o temeljnim pravima (pravu na poštovanje privatnog života i komuniciranja, pravu na zaštitu osobnih podataka i pravu na slobodu izražavanja).

Na razini EU-a nastavljaju se daljnje rasprave, no u čekanju rješenja države članice su itekako svjesne da velika većina njih ima na snazi propise koji su u proturječju sa sudskom praksom Suda EU, neke uopće nemaju nacionalno zakonodavstvo, dok su neke donijele nove propise koji se trenutačno ponovno propituju od strane njihovih nacionalnih sudova.

Države članice koje su poduzele daljnje aktivnosti suočile su se s izazovom postizanja odgovarajuće ravnoteže između poštovanja njihove obveze zaštite života i integriteta (sigurnosti) njihovih građana od sve većih prijetnji i poštovanja privatnosti tih istih građana u skladu s europskim standardima[37].

Dosadašnjim radom radne skupine Prijatelja Predsjedništva unutar Vijeća Europske unije mapirano je stanje u državama članicama, raspravljene su različite značajke presuda Suda EU i istražuju se različiti smjerovi mogućeg rješavanja ovog važnog pitanja. Najveći problem na nacionalnim razinama predstavlja tumačenje *Tele2* presude po kojoj zadržavanje podatka mora imati točno određen cilj i svrhu te točno određenu osobu ili više njih odnosno mišljenje je da se sa zadržavanjem podataka trebalo započeti tek po saznanju za neko kazneno djelo koje je počinjeno ili da zadržavanje podataka može biti usmjereno na jedno specifično zemljopisno područje na kojem je evidentiran povećan broj teških kaznenih djela za koja je zadržavanje i pristup podacima moguć[38]. Ono što ovakvo tumačenje ne uzima u obzir jest to kako je vrlo često žrtva prvi korak, koji tijela za provedbu zakonodavstva trebaju napraviti, a da bi došla do počinitelja te da svakom kaznenom djelu prethode događaji prije njega samog, poput pripreme, organizacije, promatranja i poticanja, a tom prilikom se, u pravilu, ostavljaju tragovi u digitalnom okruženju.

Sud EU-a u predmetu *Breyer*[39] donio je još jednu važnu presudu kojom se ispituje mogu li se podaci o dinamičnim adresama internetskih protokola (IP) smatrati osobnim podacima, i može li iskazivanje zakonitog interesa biti dovoljno za opravdanje pohranjivanja i obrade osobnih podataka ili to može biti učinjeno samo za specifične svrhe navedene u (sada poništenoj) Direktivi za zadržavanje podataka. Sud EU-a je zaključio da takve adrese mogu

---

[36] Ibid., točka 9.

[37] Na to je posebno upozorio Jean-Claude Juncker, predsjednik Europske komisije, u svom govoru o stanju Unije, vidi: European Commission, Juncker, J.-C. (2016), State of the Union, Bruxelles, 14. rujna 2016., poglavlje: PREMA BOLJOJ EUROPI – EUROPI KOJA ŠTITI, OSNAŽUJE I BRANI, dostupna i verzija na hrvatskom jeziku https://ec.europa.eu/commission/state-union-2016_en, (pristup 3. prosinca 2017.).

[38] Vidi presude Suda EU u spojenim presudama C-203/15 i C-698/15 (*Tele2 i Watson*), točka 119.

[39] Sud EU, *Patrick Breyer v. Bundesrepublik Deutschland*, Presuda Suda (drugo vijeće) od 19. listopada 2016. ("Zahtjev za prethodnu odluku – Obrada osobnih podataka – Direktiva 95/46/EZ – Članak 2. točka (a) – Članak 7. točka (f) – Pojam 'osobni podaci' – Adrese internetskog protokola – Pohranjivanje koje provodi pružatelj usluga internetskih medija – Nacionalni propis koji ne omogućuje da nadzornik uzme o obzir postavljeni zakoniti interes") u predmetu C-582/14.

predstavljati osobne podatke tamo gdje se osoba može identificirati, čak i u slučajevima kada treća strana mora prikupiti dodatne podatke kako bi se identifikacija izvršila[40]. Sud je također smatrao da je zadržavanje podataka dopušteno sve dok operatori *web* stranica nastoje ostvariti zakoniti interes pri zadržavanju i korištenju osobnih podataka njihovih posjetitelja. To je od velike važnosti za pravila za zadržavanje podataka jer iz toga slijedi da pružatelji usluga internetskih medija mogu zakonito pohraniti osobne podatke njihovih posjetitelja u svrhu ostvarivanja zakonitog interesa, a ne samo u svrhe koje su bile prethodno navedene u poništenoj Direktivi za zadržavanje podataka. Stoga su osnove koje opravdavaju zadržavanje podataka postale šire.

Zaista je potrebno nastaviti rad u smjeru pozitivnog rješavanja ovog pitanja u interesu sigurnosti svih građana, kao i na uvođenju svih eventualnih dodatnih zaštitnih mjera koje neće ugroziti operativnost i reakciju policijskih snaga kod provođenja kriminalističkih istraživanja i spašavanja života u kriznim situacijama.

LITERATURA

1. *Borba EU-a protiv terorizma, dostupno nahttp://www.consilium.europa.eu/hr/policies/fight-against-terrorism/,* (pristup 3. studenoga 2017.); TESAT, EUROPEAN UNION TERRORISM SITUATION AND TREND REPORT 2017, Europol, 2017., str. 10., Izvješće u obliku PDF-a dostupno na http://www.consilium.europa.eu/hr/policies/fight-against-terrorism/, (pristup 3. studenoga 2017.).
2. *Deutsche Welle, Brussels bombing aftermath - live updates*, dostupno na http://www.dw.com/en/brussels-bombing-aftermath-live-updates/a-19135323, (pristup 2. studenoga 2017.).
3. *DIREKTIVA (EU) 2016/680 EUROPSKOG PARLAMENTA I VIJEĆA od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka od strane nadležnih tijela u svrhe sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Okvirne odluke Vijeća 2008/977/PUP*.
4. *Europska komisija, KOMUNIKACIJA KOMISIJE EUROPSKOM PARLAMENTU I VIJEĆU, Jači i pametniji informacijski sustavi za granice i sigurnost, COM(2016) 205 final*, Bruxelles, 6. travnja 2016., dostupno na http://eur-lex.europa.eu/legal-content/HR/TXT/?uri=CELEX:52016DC0205, (pristup 2. studenoga 2017.).
5. *Europska komisija, KOMUNIKACIJA KOMISIJE EUROPSKOM PARLAMENTU I VIJEĆU o Akcijskom planu za jačanje borbe protiv financiranja terorizma*, COM/2016/050 final, Bruxelles, 2. veljače 2016., dostupno na http://eur-lex.europa.eu/resource.html?uri=cellar:e6e0de37-ca7c-11e5-a4b5-01aa75ed71a1.0023.02/DOC_1&format=PDF, (pristup 2. studenoga 2017.).
6. *Europska komisija, KOMUNIKACIJA KOMISIJE EUROPSKOM PARLAMENTU I VIJEĆU, Provedba Europskog programa sigurnosti: Akcijski plan EU-a za borbu protiv nezakonite trgovine vatrenim oružjem i eksplozivima te njihove uporabe*, COM/2015/0624 final, Bruxelles, 2. prosinca 2015., dostupno na http://eur-lex.europa.eu/legal-content/HR/TXT/?uri=CELEX:52015DC0624#footnote3, (pristup 2. studenoga 2017.)

[40] Ibid., para. 49.; U studenome 2016. slično je zaključio i francuski Kasacijski sud da IP adrese predstavljaju osobne podatke, France, Court of Cassation (Cour de Cassation), Arrêt No. 1184 du 3 novembre 2016, 3. studeni 2016.

7. *Europska komisija, KOMUNIKACIJA KOMISIJE EUROPSKOM PARLAMENTU, EUROPSKOM VIJEĆU I VIJEĆU o provedbi Europskog programa sigurnosti za borbu protiv terorizma i stvaranje uvjeta za uspostavu učinkovite i istinske sigurnosne Unije*; ANNEX 1, PRILOG KOMUNIKACIJI KOMISIJE EUROPSKOM PARLAMENTU, EUROPSKOM VIJEĆU I VIJEĆU o provedbi Europskog programa sigurnosti za borbu protiv terorizma i stvaranje uvjeta za uspostavu učinkovite i istinske sigurnosne unije, COM/2016/230 final, Bruxelles, 20. travnja 2016., dostupno na http://eur-lex.europa.eu/legal-content/HR/TXT/?uri=CELEX:52016DC0230, (pristup 2. studenoga 2017.).
8. *Europska komisija, KOMUNIKACIJA KOMISIJE EUROPSKOM PARLAMENTU, VIJEĆU, EUROPSKOM GOSPODARSKOM I SOCIJALNOM ODBORU I ODBORU REGIJA Europski program sigurnosti*, COM(2015) 185 final, Strasbourg, 28. travnja 2015., dostupno na http://eur-lex.europa.eu/legal- content/HR/ALL/?uri=CELEX:52015DC0185, (pristup 2. studenoga 2017.).
9. *Europska komisija, KOMUNIKACIJA KOMISIJE EUROPSKOM PARLAMENTU, VIJEĆU, EUROPSKOM GOSPODARSKOM I SOCIJALNOM ODBORU I ODBORU REGIJA, Sprječavanje radikalizacije koja dovodi do terorizma i nasilnog ekstremizma: Jačanje odgovora Europske unije*, COM(2013) 941 final, Bruxelles, 15. siječnja 2014., dostupno na https://ec.europa.eu/transparency/regdoc/rep/1/2013/HR/1-2013-941-HR-F1-1.Pdf (pristup 3. studenoga 2017.).
10. *Mišljenje Suda (Veliko vijeće) od 26. srpnja 2017. – Europski parlament (mišljenje 1/15), (Mišljenje na temelju članka 218. stavka 11. UFEU-a – Prijedlog sporazuma između Kanade i Europske unije – Prijenos podataka iz popisa imena zrakoplovnih putnika iz Unije u Kanadu – Odgovarajuće pravne osnove – Članak 16. stavak 2., članak 82. stavak 1. drugi podstavak točka (d) i članak 87. stavak 2. točka (a) UFEU-a – Usklađenost sa člancima 7. i 8. te člankom 52. stavkom 1. Povelje Europske unije o temeljnim pravima),* dostupno na http://curia.europa.eu/juris/document/document.jsf?docid=194498&mode=req&pageIndex=1&dir=&occ=first&part=1&text=&doclang=HR&cid=73014#1, (pristup 4. rujna 2017.).
11. *Pravilnik o vojnopolicijskim poslovima i provedbi ovlasti ovlaštenih službenih osoba Vojne policije*, NN broj: 44/2014.
12. *Presuda Suda (Veliko vijeće) od 21. prosinca 2016.,* Tele2 Sverige AB i Secretary of *State for the Home Department protiv Post- och telestyrelsen i dr. (zahtjevi za prethodnu odluku koje su uputili Kammarrätten i Stockholm i Court of Appeal (England & Wales) (Civil Division), „Zahtjev za prethodnu odluku – Elektroničke komunikacije – Obrada osobnih podataka – Povjerljivost elektroničkih komunikacija – Zaštita – Direktiva 2002/58/EZ – Članci 5., 6. i 9. i članak 15. stavak 1. – Povelja Europske unije o temeljnim pravima – Članci 7., 8. i 11. i članak 52. stavak 1. – Nacionalno zakonodavstvo – Pružatelji elektroničkih komunikacijskih usluga – Obveza koja se odnosi na opće i neselektivno zadržavanje podataka o prometu i podataka o lokaciji – Nacionalna tijela – Pristup podacima – Nepostojanje prethodnog nadzora suda ili nadzora neovisnog upravnog tijela – Usklađenost s pravom Unije.“,* (spojeni predmeti C-203/15 i C-698/15), dostupno na http://eur-lex.europa.eu/legal-content/HR/TXT/?uri=CELEX%3A62015CJ0203#t-ECR_62015CJ0203_HR_01-E0001, (pristup 1. studenoga 2017.).
13. *Prijedlog UREDBE EUROPSKOG PARLAMENTA I VIJEĆA o poštovanju privatnog života i zaštiti osobnih podataka u elektroničkim komunikacijama te stavljanju izvan snage Direktive 2002/58/EZ (Uredba o privatnosti i elektroničkim komunikacijama),* COM(2017) 10 final, Bruxelles, 10. siječnja 2017., dostupno na: http://eur-lex.europa.eu/legal-content/HR/TXT/?uri=CELEX%3A52017PC0010, (pristup 29. studenog 2017.).
14. *Službeni list Europske unije, C 175/6, 10. lipnja 2014., Presuda Suda (veliko vijeće) od*

8. travnja 2014. (zahtjev za prethodnu odluku koji su uputili High Court of Ireland, Verfassungsgerichtshof – Irska, Austrija) – Digital Rights Ireland Ltd (C-293/12), Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl i dr. (C-594/12) protiv 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 (Spojeni predmeti C-293/12 i C-594/12).

15. *Službeni list Europske unije, L 105/54, 13. travnja 2004., DIREKTIVA 2006/24/EZ EUROPSKOG PARLAMENTA I VIJEĆA od 15. ožujka 2006. o zadržavanju podataka dobivenih ili obrađenih u vezi s pružanjem javno dostupnih elektroničkih komunikacijskih usluga ili javnih komunikacijskih mreža i o izmjeni Direktive 2002/58/EZ.*
16. *Službeni list Europske unije, L 119/1, 4. svibnja 2016., UREDBA (EU) 2016/679 EUROPSKOG PARLAMENTA I VIJEĆA od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka).*
17. *Službeni list Europske unije, L 119/132, 4. svibnja 2016., DIREKTIVA (EU) 2016/681 EUROPSKOG PARLAMENTA I VIJEĆA od 27. travnja 2016. o uporabi podataka iz evidencije podataka o putnicima (PNR) u svrhu sprečavanja, otkrivanja, istrage i kaznenog progona kaznenih djela terorizma i teških kaznenih djela*.
18. *Službeni list Europske unije, L 119/89, 4. svibnja 2016., DIREKTIVA (EU) 2016/680 EUROPSKOG PARLAMENTA I VIJEĆA od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka od strane nadležnih tijela u svrhe sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Okvirne odluke Vijeća 2008/977/PUP.*
19. *Sud EU, Patrick Breyer v. Bundesrepublik Deutschland, Presuda Suda (drugo vijeće) od 19. listopada 2016. („Zahtjev za prethodnu odluku – Obrada osobnih podataka – Direktiva 95/46/EZ – Članak 2. točka (a) – Članak 7. točka (f) – Pojam ¢osobni podaci¢ – Adrese internetskog protokola – Pohranjivanje koje provodi pružatelj usluga internetskih medija – Nacionalni propis koji ne omogućuje da nadzornik uzme o obzir postavljeni zakoniti interes") u predmetu C-582/14.*
20. *Sud Europske unije, PRIOPĆENJE ZA MEDIJE br. 54/14, Luxembourg, 8. travnja 2014., Presuda u spojenim predmetima C-293/12 i C-594/12 Digital Rights Ireland i Seitlinger* i dr., dostupno na https://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp-140054hr.pdf, (pristup 29. studenog 2017.).
21. *United Nations (UN), Human Rights Council, Cannataci, J. (2016), Report of the Special Rapporteur on the right to privacy, A/HRC/31/64*, 8. ožujka 2016., str. 9., točka 23., dostupno na https://documents-dds-ny.un.org/doc/UNDOC/GEN/G16/262/26/PDF/G1626226.pdf?OpenElement, (pristup 3. prosinca 2017.).
22. *UREDBA (EU) 2016/679 EUROPSKOG PARLAMENTA I VIJEĆA od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ* (Opća uredba o zaštiti podataka).
23. *Uredba o obvezama iz područja nacionalne sigurnosti Republike Hrvatske za pravne i fizičke osobe u telekomunikacijama*, NN broj: 83/03., 64/08. i 76/2013.
24. Vi*jeće Europe, Odbor ministara* (2016), *Preporuka CM/Rec* (2016)5 Odbora ministara državama članicama o slobodi interneta, 13. travnja 2016., točka 4.1.7.
25. *Vijeće Europske unije 2014., Revidirana Strategija EU-a za borbu protiv radikalizacije i novačenja terorista*, dokument broj 9956/14.
26. *Vijeće Europske unije 2014., Zaključci Vijeća o razvoju obnovljene strategije unutarnje sigurnosti Europske unije, Bruxelles*, 4. prosinca 2014., dokument 15670/14, str. 13., dostu-

pan na http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2015670%202014%20INIT

27. *Vijeće sigurnosti, Resolution 1373(2001), UN Doc. S/RES/1373 (2001) od 28. rujna 2001., Vijeće sigurnosti, Report of the Policy Working Group on the United Nations and Terrorism*, UN Doc. A/57/273-S/2002/875.
28. *Zakon o elektroničkim komunikacijama*, NN broj: 73/08., 90/11., 133/12., 80/13. i 71/14.
29. *Zakon o kaznenom postupku*, NN broj: 110/97., 58/02., 152/08., 76/09., 80/11., 121/11., 91/12., 143/12., 56/13., 145/13. i 152/14.
30. *Zakon o obrani*, NN broj: 73/13.
31. *Zakon o policijskim poslovima i ovlastima*, NN broj: 76/09. i 92/14.
32. *Zakon o sigurnosno-obavještajnom sustavu Republike Hrvatske*, NN broj: 79/06. i 105/06.
33. *Zakon o sigurnosno-obavještajnom sustavu Republike Hrvatske*, NN broj: 79/06. i 105/06.
34. *Zakon o telekomunikacijama*, NN broj: 122/03.
35. Zrinka Salaj, *Međunarodnopravne implikacije masovnog nadzora elektroničkih komunikacija u kontekstu ljudskih prava, s posebnim osvrtom na sigurnosno-obavještajni sustav u Republici Hrvatskoj*, ZPR 6(1) 2017., str. 15.-40.

Summary

Jelena Levak, Damir Osterman

Protection, Retention and Exchange of Data Used by LEAs – Possible Technical Solutions for Data Retention After CJEU Annulled Data Retention Directive

Law enforcement authorities must have the appropriate data retention tool to be able to, somehow, maintain the status quo in counter terrorism and serious crime. At the EU level, data retention is an absolute basic element in this fight, but there must be an appropriate balance between fundamental rights, the right to privacy and the protection of personal data and further work on the security of citizens. The further possibility of data retention is of paramount importance for the safety of citizens, especially in terms of prevention, investigation, detection and prosecution of criminal offenses, and defence and protection of public and national security. On the other hand, the retention of data constitutes a restriction of human rights guaranteed by the EU Charter of Fundamental Rights (the right to respect for private life and communication, the right to protection of personal data and the right to freedom of expression).

The goal of this paper is to present the history of EU legislation with which the EU is trying to tackle the issues of counter terrorism and data protection reform which immediately after the attacks resulted in a package of various legislative solutions, the judgement of the Court of Justice of the European Union regarding Data Retention Directive and its annulment, and the current situation in the discussion that followed the annulment.

From a technical point of view, the possibilities of harmonizing, collecting, processing and storing large amounts of data that can be used to identify persons will be presented, where as such, they must be aligned with the General Data Protection Regulation and the so-called „Police Directive".

As data protection measures, in the sense of the above-mentioned regulation, encryption, anonimyzation and pseudonymization will be elaborated in the paper, taking into account their advantages and disadvantages. In addition, the paper will present the data handling - related legislation and the concept of technical solution that could restrict data processing and provide supervision regarding the handling of data.

Key words: data retention, right to respect for private life and communication, encryption, pseudonymization, anonymization.