UDK: 342.738:004.3/.4(4)EU
341.645(4)EU:004.3/.4
Primljeno: veljača 2018.
Pregledni znanstveni rad

Dr. sc. Kristian Turkalj [*]
Daška Leppee Pažanin, dipl. iur. [**]

IZAZOVI PRAVNOG UREĐENJA ZADRŽAVANJA PODATAKA ELEKTRONIČKE KOMUNIKACIJE U SVJETLU NEDAVNE PRAKSE SUDA EU-A

Pravno uređenje područja zadržavanja telekomunikacijskih podataka već je nekoliko godina među najaktualnijim pitanjima u Europskoj uniji u vezi s postizanjem ravnoteže između osiguravanja sigurnosti poduzimanjem mjera borbe protiv terorizma i organiziranog kriminala te osiguranja zaštite ljudskih prava i temeljnih sloboda. Nakon terorističkih napada u SAD-u i Europi početkom prošlog desetljeća pojavila se prijeka potreba za uvođenjem obveze prikupljanja i zadržavanja podataka elektroničke komunikacije radi učinkovitije borbe protiv terorizma i teških kaznenih djela. Zakonodavne inicijative na razini Europske unije rezultirale su donošenjem propisa kojima se postavlja okvir režima zadržavanja podataka. Nesporno je da je zadržavanje podataka elektroničke komunikacije iznimno korisno i učinkovito sredstvo za sprječavanje, otkrivanje, istraživanje i progon kaznenih djela. Istodobno, ono je iznimno „invazivno" zadiranje u temeljna prava i slobode pojedinaca. Posebice zadire u pravo na privatnost te pravo na slobodu izražavanja zajamčena Poveljom o temeljnim pravima. Sud Europske unije u svojim je presudama Digital Rights i Tele2 upozorio na kršenje temeljnih prava u europskim i nacionalnim propisima koji se odnose na zadržavanje podataka. U tekstu se analiziraju dosezi predmetnih presuda na nacionalno zakonodavstvo te ključni standardi zaštite ljudskih prava u vezi sa zadržavanjem podataka na koje je upozorio Sud EU-a u svojim odlukama. Nakon presuda Suda EU-a države članice EU-a, uključujući i RH, našle su se pred velikim izazovom unaprjeđenja pravnog okvira zadržavanja podataka. U tom se smislu analizira relevantan domaći pravni okvir kao i potreba preispitivanja pojedinih rješenja radi potpune usklađenosti sa zahtjevima i kriterijima koje je postavio Sud EU-a.[1]

***Ključne riječi**: EU,* acquis, *zadržavanje podataka, Sud EU-a, Direktiva o zadržavanju podataka, prometni podatci, tajnost komunikacija, sigurnost, terorizam, privatnost, zaštita osobnih podataka*

---

[*] Dr. sc. Kristian Turkalj, Ministarstvo pravosuđa (*Ministry of Justice*), Ulica grada Vukovara 49, Zagreb
ORCID ID: orcid.org/0000-0002-7998-6874.

[**] Daška Leppee Pažanin, dipl. iur., Ministarstvo pravosuđa (*Ministry of Justice*), Ulica grada Vukovara 49, Zagreb, daska.leppee@pravosudje.hr.
ORCID ID: orcid-org/0000-0002-4908-663X

[1] Stavovi izneseni u ovom radu isključivo su stavovi autora i ne mogu se poistovjetiti sa službenim stavovima institucije u kojoj su autori zaposleni.

1. UVOD

Potreba za uvođenjem obveze prikupljanja i zadržavanja podataka elektroničke komunikacije radi učinkovitije zaštite javne i nacionalne sigurnosti te borbe protiv terorizma, organiziranog kriminala i teških kaznenih djela u državama članicama Europske unije aktualizirana je još 90-ih godina prošlog stoljeća[2] kada su tijela progona upozorila na činjenicu da je zbog nedostatnih zadržanih podataka elektroničke komunikacije uspješnost kaznenog progona suočena s nerazmjernim poteškoćama.

Ključni događaji koji su utjecali na normativno uređenje područja zadržavanja podataka elektroničke komunikacije u Europskoj uniji bili su teroristički napadi u Sjedinjenim Američkim državama, Madridu i Londonu.[3] Navedeni teroristički napadi doveli su do promjene javne svijesti te su pitanjima sigurnosti dali prednost u odnosu na zaštitu ljudskih prava. Prepoznavši važnost zadržavanja podataka elektroničke komunikacije u borbi protiv terorizma i teških kaznenih djela, europski zakonodavac poduzeo je konkretne mjere propisivanjem obveze pružatelja elektroničkih komunikacijskih usluga i javnih komunikacijskih mreža (dalje u tekstu: pružatelji usluga) da pohranjuju podatke u elektroničkim komunikacijama svih svojih korisnika u određenom razdoblju te da osiguraju da tako zadržani podatci budu raspoloživi nadležnim tijelima radi zaštite obrane i nacionalne sigurnosti te istrage, otkrivanja i kaznenog progona kaznenih djela. U tom su kontekstu 2002. i 2006. godine prihvaćeni zakonodavni instrumenti koji su regulirali režim zadržavanja podataka – Direktiva o privatnosti i elektroničkim komunikacijama[4] i Direktiva o zadržavanju podataka.[5]

Međutim, u travnju 2014. godine Sud Europske unije donio je presudu *Digital Rights*[6] kojom je proglasio nevaljanom Direktivu o zadržavanju podataka, jedini instrument koji je na razini Europske unije cjelovito regulirao pitanje zadržavanja podataka. Sud je stavio Direktivu izvan snage jer je smatrao da se ona osobito teško miješa u temeljna prava poštovanja privatnog života i zaštite osobnih podataka.

Korak dalje otišla je presuda *Tele2* istog suda iz prosinca 2016. godine[7] prema kojoj države članice ne mogu pružateljima elektroničkih komunikacijskih usluga namet-

[2] *Dragičević; Gumzej*, 2014, 39–79.

[3] Više o utjecaju terorističkih napada na razvoj politike Europske unije u borbi protiv terorizma vidi *Turkalj*, 2011, 82–101.

[4] Direktiva 2002/58/EZ Europskog Parlamenta i Vijeća od 12. srpnja 2002. o obradi osobnih podataka i zaštiti privatnosti u području elektroničkih komunikacija (SL L 201, 31. 7. 2002.), 37–47.

[5] 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 (SL L 105, 2006.), 54–63.

[6] Vidi presudu Suda (Veliko vijeće) od 8. travnja 2014. (spojeni predmeti C-293/12 i C-594/12); Zbornik sudske prakse.

[7] Vidi presudu Suda (Veliko vijeće) od 21. prosinca 2016. (spojeni predmeti C-203/15 i C-698/15); Zbornik sudske prakse.

nuti opću obvezu zadržavanja podataka, odnosno prema kojoj se pravu Unije protive nacionalni propisi država članica EU-a koji nalažu opće i neselektivno zadržavanje podataka.

Takva praksa Suda proizvela je dalekosežne učinke jer na razini Europske unije više ne postoje harmonizirana pravila o zadržavanju podataka elektroničke komunikacije kao ni pravila o pristupu tim podatcima te istodobno izostaje ujednačena zaštita prava građana EU-a. Države članice Europske unije ostale su bez europskog okvira koji bi postavio jasne smjernice za nacionalne režime zadržavanja podataka, što je dovelo do različitih situacija u državama članicama. U nekim su državama članicama ustavni sudovi ukinuli nacionalne propise koji uređuju ovo područje, dok su neke države članice samoinicijativno zadržale postojeće nacionalne okvire ili stvorile nove nacionalne okvire zadržavanja podataka koji su, bez postojanja minimalnih pravila zajedničkih za sve države članice u ovom području, međusobno neujednačeni i nedosljedni.

Osnovna su pitanja na koja je potrebno odgovoriti u pronalasku odgovarajućeg rješenja u vezi sa zadržavanjem podataka elektroničke komunikacije kako pomiriti zahtjeve i kriterije koje postavlja Sud Europske unije u odnosu na zaštitu temeljnih ljudskih prava s jedne strane i potrebe nadležnih službi za otkrivanje, sprječavanje i progon terorizma i organiziranog kriminala s druge strane, kako konstruirati dopustiv zakonodavni okvir s obzirom na to da pravo Unije dopušta da države članice preventivno propišu ciljano zadržavanje podataka elektroničke komunikacije radi borbe protiv teških kaznenih djela uz uvjet da takvo zadržavanje – kad je riječ o kategorijama podataka koje treba zadržati, predviđenim sredstvima komunikacije, osobama na koje se odnosi i trajanju primijenjenog zadržavanja – bude ograničeno na ono što je strogo nužno, a pristup nacionalnih tijela tim podatcima podvrgnut prethodnom nadzoru neovisnoga tijela, uz dodatna zaštitna jamstva osobnih podataka koji se zadržavaju.

2. ZAŠTITA JAVNOG I PRIVATNOG INTERESA KAO DVAJU SUPROTSTAVLJENIH PRAVA

Za represivna tijela zadržavanje telekomunikacijskih podataka iznimno je koristan alat u zaštiti nacionalne sigurnosti i javnog interesa. Ono omogućuje otkrivanje, sprječavanje, istraživanje i procesuiranje terorizma i teških kaznenih djela. Stoga ima i preventivnu i represivnu svrhu. No, s druge strane, zadržavanje podataka zadire u temeljna prava i slobode građana zajamčena međunarodnim pravnim instrumentima. Što se tiče zaštite ljudskih prava, za države članice EU-a posebice su relevantne Konvencija o zaštiti ljudskih prava i temeljnih sloboda te Povelja Europske unije o temeljnim pravima (dalje u tekstu: Povelja).

Povelja potvrđuje prava koja proizlaze osobito iz ustavnih tradicija i međunarodnih obveza zajedničkih državama članicama, iz Europske konvencije za zaštitu ljudskih prava i temeljnih sloboda, iz socijalnih povelja koje su prihvatile Unija i Vijeće Europe te iz prakse Suda Europske unije i Europskog suda za ljudska prava. Povelja je primarno pravo EU-a te ima jednaku pravnu obvezatnost za države članice kao što je imaju i sami osnivački ugovori EU-a. U odnosu na zadržavanje podataka važno je istaknuti da Povelja svakomu jamči pravo na poštivanje privatnog i obiteljskog života, doma i komuniciranja (čl. 7.), pravo na zaštitu osobnih podataka (čl. 8.) te pravo na slobodu izražavanja koje uključuje slobodu mišljenja i primanja i širenja informacija i ideja bez miješanja tijela javne vlasti i bez obzira na granice (čl. 11.). Spomenuta prava mogu biti ozbiljno povrijeđena zadržavanjem podataka. Naime, iz zadržanih podataka može se dobiti vrlo poman uvid u privatni život pojedinca te zbog straha od praćenja oni mogu biti suzdržani od komunikacije i izražavanja sredstvima komunikacija.

Premda su navedena temeljna prava zajamčena i zaštićena, ona ipak nisu neograničena i apsolutna. Prema članku 8., st. 2. Europske konvencije za zaštitu ljudskih prava i temeljnih sloboda, kao i tumačenju Europskog suda za ljudska prava, javna vlast neće se miješati u ostvarivanje zajamčenih prava (npr. pravo na privatni život) osim kada je to u skladu sa zakonom i ako je nužno u demokratskom društvu radi interesa državne sigurnosti, javnog reda i mira, gospodarske dobrobiti zemlje, sprječavanja nereda ili zločina, zaštite zdravlja ili morala odnosno radi zaštite prava i sloboda drugih. Dakle, države mogu poduzimati mjere kojima će ograničiti temeljna prava radi zaštite pojedinih interesa. No, 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.[8] Ograničenje mora biti nužno u demokratskom društvu i mora se provoditi isključivo radi ispunjenja legitimna cilja. Mjerom se mora zadovoljiti vrlo važna, neodgodiva socijalna potreba da se ispuni legitiman cilj, pri čemu ona mora biti razmjerna u odnosu na taj cilj pa tako uvijek treba razmotriti može li se on postići mjerom kojom se u manjem opsegu zadire u temeljno pravo.

Nije sporno da pravo Europske unije dopušta odstupanja od apsolutne zaštite temeljnih ljudskih prava kada je to nužno za zaštitu drugih legitimnih interesa. Međutim, sporno je jesu li određene mjere kojima se ograničavaju temeljna prava razmjerne i nužne da bi se ostvario koji legitimni cilj. Potrebno je imati na umu da Povelja, osim navedenih prava, jamči svim građanima EU-a i pravo na osobnu sigurnost (čl. 6.). Iako postoji visokorazvijena svijest o važnosti zaštite tih interesa, odnosno, između ostalog, i osiguranja područja slobode i sigurnosti za građane EU-a, posebno u kontekstu suvremene i aktualne borbe protiv terorizma i kriminala, očito je

[8] Više o tome u smislu predvidljivosti vidi *Stoeva*, 2014, 579–580.

da zaštita prava na poštivanje privatnog i obiteljskog života, doma i komuniciranja kao i prava na zaštitu osobnih podataka te prava na slobodu izražavanja postaje sve važnija u odnosu na potrebu za osiguranjem europskog područja sigurnosti. Gdje povući crtu razdvajanja između ovih dvaju suprotstavljenih prava, jedno je od najtežih pitanja za zakonodavce na europskoj i nacionalnoj razini. Potrebno je upitati jesu li ljudska prava važnija od nacionalne sigurnosti i borbe protiv terorizma i teških kaznenih djela, je li potrebno odrediti koje od ovih dvaju prava ima prednost ili je moguće postići njihovu komplementarnost, odnosno ima li smisla štititi slobode i ljudska prava umanjivanjem slobode i ljudskih prava. Sva navedena pitanja otvaraju raspravu o vrijednostima koje moraju prevagnuti u demokratskom društvu te u konačnici o tome u kakvu društvu želimo živjeti.[9]

U tom je smislu svakako izazov osigurati pravilnu ravnotežu između sigurnosti i ljudskih prava, odnosno odrediti kako uravnotežiti interes Europske unije što se tiče potpuno zajamčene sigurnosti i borbe protiv najsuvremenijih oblika terorizma i organiziranog kriminala s jedne strane i prava na poštivanje privatnog života građana i posebno na zaštitu njihovih osobnih podataka s druge strane, kao temeljnih prava koja uživaju osobitu važnost svakoga demokratskog i pluralističkog društva te su dio vrijednosti na kojima počiva Unija. Sud EU-a u svojim je presudama u vezi sa zadržavanjem podataka postavio smjernice kojima bi trebalo ostvariti razmjernost u ograničavanju temeljnih prava radi zaštite ostalih legitimnih ciljeva.

Uvažavajući zaključke Suda u odnosu na potrebu punog poštivanja temeljnih prava zajamčenih Poveljom, smatramo da je i predloženim rješenjima, kojima bi se zadovoljilo načelo proporcionalnosti nacionalnog propisa o zadržavanju podataka, potrebno pristupiti s osobitom pozornošću. Naime, i one mjere koje se predlažu kao potrebne, odgovarajuće i razmjerne moraju biti u skladu s temeljnim pravima koje jamči Povelja. Potrebno je izbjeći situacije gdje bi se u skladu s presudom Suda EU-a zaštitila pojedina prava iz čl. 7. i 8. Povelje, ali na štetu nekih drugih prava također zajamčenih Poveljom. Primjerice, prema presudi *Tele2* ograničenje temeljnih prava može se osigurati kada nadležna nacionalna tijela na temelju objektivnih elemenata utvrde da na jednom ili više zemljopisnih područja postoji pojačana opasnost od pripremanja ili počinjenja takvih djela. Postavlja se pitanje eventualne povrede temeljnih prava ostalih osoba s tog područja čiji su podatci *a priori* zadržani u tome zemljopisnom skupu a da te osobe nisu ni prethodno ni naknadno dovedene u vezu s pripremanjem ili počinjenjem kaznenih djela. Ograničenje na određeno zemljopisno područje ili pak određena sredstva komunikacije moglo bi rezultirati preusmjeravanjem aktivnosti povezanih s teškim kaznenim djelima na zemljopisna područja i/ili sredstva komunikacije koja nisu obuhvaćena sustavom nadzora, odnosno moglo

[9] „Informacije i podaci: Pogled u budućnost", 5. međunarodna znanstvena konferencija Petar Šarčević, Opatija, 6. i 7. listopada 2017.

bi dovesti do situacije da potencijalni počinitelji slobodno i bez nadzora djeluju izvan nadziranih područja, to jest mijenjaju svoja područja djelovanja. Također, potrebno je imati u vidu i činjenicu da aktualni teroristički napadi vrlo često nisu pripremani na području na kojem je izveden teroristički napad niti su počinjeni na usku zemljopisnom području da bi nadležna tijela s lakoćom mogla primijeniti zemljopisni kriterij.

Imajući sve navedeno u vidu, u idućem će razdoblju biti potrebno pronaći zadovoljavajuća rješenja kojima će se postići puno poštivanje temeljnih prava koje građanima jamči Povelja Europske unije o temeljnim pravima uz istodobno osiguranje tijelima kaznenog progona svih nužnih alata od temeljna značenja za istraživanje kriminala. Pri tome je važno imati na umu da bi svako veće ograničenje opće obveze zadržavanja podataka moglo rezultirati izuzimanjem iz zadržavanja onih podataka koji bi mogli biti relevantni, čime bi se znatno umanjila korisnost tog sustava u borbi protiv teških kaznenih djela.

3. VAŽNOST ZADRŽAVANJA PODATAKA ZA RAD TIJELA KAZNENOG PROGONA

Važnost zadržavanja podataka elektroničke komunikacije za borbu protiv svih suvremenih pojavnih oblika terorizma i teških kaznenih djela nesporna je. Zadržani podatci imaju iznimno važnu ulogu u procesuiranju kaznenih djela i u preventivnom djelovanju u borbi protiv terorizma i organiziranog kriminala zbog otkrivanja mreže mogućih počinitelja kaznenog djela.[10] Također, zadržavanje podataka može imati važnu ulogu i izvan okvira borbe protiv terorizma i organiziranog kriminala, primjerice u potrazi za nestalim osobama gdje podatci o posljednjoj komunikaciji mogu imati ključnu ulogu u istrazi. Također, ti su podatci pokazali svoju dokaznu važnost kao alibi u postupku dokazivanja nevinosti.

Zadržani podatci pružaju tijelima kaznenog progona dodatno sredstvo istrage na temelju kojeg mogu spriječiti ili razjasniti teška kaznena djela. Takva mjera, za razliku od ciljanih mjera nadzora, omogućuje tijelima kaznenog progona da uvidom u zadržane podatke „promatraju prošlost" osoba na koje se odnose. Mjere ciljanog nadzora usredotočene su na osobe koje su već identificirane kao potencijalno povezane, čak i neizravno ili slabo, s teškim kaznenim djelima. Takve ciljane mjere omogućuju nadležnim tijelima da pristupe podatcima koji se odnose na komunikaciju takvih osoba te čak i da pristupe sadržaju njihove komunikacije. Međutim, taj je pristup ograničen samo na komunikaciju nakon što su osobe identificirane. S druge strane, opća obveza zadržavanja podataka odnosi se na cjelokupnu komunikaciju svih korisnika, pri čemu nije potrebno da su oni ikako povezani s teškim kaznenim djelima. Takva obveza omogućuje nadležnim tijelima pristup povijesti komunikaci-

[10] O tome govori i *Vaciago*, 2014, 66.

je osoba koje još nisu identificirane kao potencijalno povezane s teškim kaznenim djelima. U tom smislu, opća obveza zadržavanja podataka daje tijelima kaznenog progona određenu mogućnost promatranja prošlosti jer im omogućuje pristup komunikaciji takvih osoba prije nego što su tako identificirane. Drugim riječima, korisnost opće obveze zadržavanja podataka u borbi protiv teških kaznenih djela leži u toj ograničenoj mogućnosti promatranja prošlosti na temelju uvida u podatke koji se odnose na povijest komunikacije osoba prije nego što se posumnjalo u njihovu povezanost s teškim kaznenim djelima.[11]

Europska komisija podnijela je 2011. godine Izvješće o implementaciji Direktive o zadržavanju podataka u državama članicama EU-a u kojem se ističe važnost zadržavanja podataka kao vrijedna, a u mnogim slučajevima i nužna sredstva za sprječavanje kriminala i borbu protiv njega, uključujući zaštitu žrtava i oslobađanje nevinih osoba u kaznenom postupku.[12] Na temelju statističkih podataka i ilustrativnih primjera koje su dostavile države članice o vezi između zadržanih podataka i broja osuđujućih i oslobađajućih presuda, odnosno obustava postupaka ili sprječavanja zločina, moguće je donijeti niz zaključaka o ulozi i vrijednosti zadržanih podataka u kaznene svrhe. Primjerice, austrijska se policija samo tijekom tri mjeseca koristila zadržanim podatcima u čak 92 % provedenih istraga, dok njemačka policija za 44,5 % istraga u kojima su upotrijebljeni zadržani podatci nije imala na raspolaganju druga sredstva za provođenje istrage. U Ujedinjenom Kraljevstvu zadržani podatci bili su od odlučna značenja u većini, ako ne i u svim istragama koje su rezultirale osuđujućim presudama.

U Ujedinjenom Kraljevstvu 2012. godine provedena je studija o starosti zadržanih podataka koji su uspješno upotrijebljeni radi kaznenog progona koja je pokazala da je čak 84 % tih podataka zadržano do šest mjeseci od dana obavljene komunikacije. U većini slučajeva počinitelji kaznenih djela nisu otprije poznati policiji te su podatci o elektroničkim komunikacijama bili od presudne važnosti za prikupljanje potrebna dokaznog materijala, a time i uspješan ishod istrage. Bez zadržavanja podataka većina počinitelja ne bi nikad bila otkrivena, odnosno procesuirana.[13]

Praksa evidentno pokazuje da postoji velik broj slučajeva koji ne bi mogli biti procesuirani zbog nedostatka zadržanih podataka, odnosno postoji velik broj slučajeva kada su zadržani podatci bili važna dodana vrijednost u kaznenim postupcima te su pridonijeli uspješnu progonu. Tijelima kaznenog progona, prema trenutačnim

[11] Mišljenje nezavisnog odvjetnika Henrika Saugmandsgaardaøea u spojenim predmetima C-203/15 Tele2 Sverige AB/Post-ochtelestyrelsen i C-698/15 Secretary of State for Home Department/Tom Watson i dr. od 19. srpnja 2016. godine, 25.

[12] *Report from the Commission to the Council and the European Parliament: Evaluation report on the Data Retention Directive (Directive 2006/24/EC), Brussels, 18.4.2011 COM(2011) 225 final*, 23–25.

[13] *Age of communications data requested (2012 ACPO SPOC survey).*

zakonodavnim rješenjima, dostupni su podatci o elektroničkim komunikacijama u odnosu na osumnjičenu, odnosno optuženu osobu tako da se ti podatci retroaktivno zadržavaju kao dio skupnih podataka zadržanih u odnosu na neograničen broj osoba te se za potrebe istrage i progona naknadno izdvajaju u odnosu na pojedinog osumnjičenika odnosno optuženika. Prema stavovima represivnog aparata teško je predvidjeti koja je osoba potencijalni počinitelj kaznenih djela da bi se samo u odnosu na nju zadržavali podatci. Zadržani podatci iznimno su važni za provođenje istrage i utvrđivanje svih sudionika u počinjenome kaznenom djelu. To je posebice očito pri progonu počinitelja terorističkih napada. Naime, nakon počinjenja kaznenog djela i saznanja osobe počinitelja, za rekonstrukciju cijele terorističke mreže od iznimne je važnosti utvrditi krug osoba s kojima je počinitelj komunicirao neposredno prije napada odnosno tijekom pripremanja kaznenog djela. Jedino će zadržani podatci moći pružiti korisne informacije o osobi i modusu počinjenja kaznenog djela kao i utvrditi s kime je počinitelj bio u intenzivnu kontaktu te tko mu je pomagao i pripremao počinjenje kaznenog djela. Zbog toga tijela kaznenog progona trebaju zadržavanje podataka da bi potpuno i učinkovito istražili zločine, pogotovo one gdje su zadržani podatci samo moguće početne točke za pokretanje istrage.

4. PRAVNI OKVIR EU-a ZA ZADRŽAVANJE PODATAKA

Još 1996. godine, vođena američkim iskustvom, Europska unija počela je intenzivne rasprave i promišljanja o uvođenju režima zadržavanja podataka elektroničke komunikacije za potrebe istraga i kaznenog progona.[14] Tadašnji pozitivni europski propisi (*Direktiva 97/66/EZ Europskog parlamenta i Vijeća od 15. prosinca 1997. o obradi osobnih podataka i zaštiti privatnosti u području telekomunikacija*) obvezivali su pružatelje usluga isključivo na zadržavanje podataka o prometu koji su nužni radi naplaćivanja usluge od pretplatnika koji su obrađeni radi prijenosa komunikacije ili obračuna i naplate troškova, a odnose se na pretplatnike ili korisnike usluga, i to na kraće od tri mjeseca. Budući da takav okvir nije zadovoljavao potrebe tijela kaznenog progona, europski zakonodavac odlučio je postaviti okvire režima zadržavanja podataka kakav danas poznajemo.

Uvođenje novih naprednih digitalnih tehnologija u javne komunikacijske mreže dovelo je do posebnih zahtjeva u vezi sa zaštitom osobnih podataka i privatnosti korisnika te je nastala potreba za donošenjem posebnih zakona i drugih propisa radi zaštite temeljnih prava i sloboda građana EU-a. Stoga je 2002. godine prihvaćena Direktiva o privatnosti i elektroničkim komunikacijama. Direktivama je cilj osigurati ujednačenu razinu zaštite temeljnih prava i sloboda, a posebno prava na privatnost

[14] *Drewry*, 2016, 732.

i povjerljivost u vezi s obradom osobnih podataka u području elektroničkih komunikacija kao i osigurati slobodan prijenos tih podataka u Europskoj uniji. Osim što nameće državama članicama obvezu da osiguraju povjerljivost komunikacija, Direktiva dopušta vrlo važnu iznimku u čl. 15., st. 1. U skladu s navedenom odredbom države članice mogu donijeti zakonske mjere kojima će ograničiti opseg pojedinih prava i obveza koje pruža Direktiva kada je takvo ograničenje nužna, prikladna i razmjerna mjera unutar demokratskoga društva radi zaštite nacionalne sigurnosti (odnosno državne sigurnosti), obrane, javne sigurnosti te radi sprječavanja, istrage, otkrivanja i progona kaznenih djela. U tom smislu države članice mogu donijeti zakonske mjere kojima se omogućuje zadržavanje podataka opravdano propisanim razlozima u ograničenom razdoblju.[15]

Ipak, budući da se Europa počela suočavati sa sigurnosnim prijetnjama i ugrozama te su uslijedili teroristički napadi na europske metropole[16], postala je jasna potreba za posebnim instrumentom koji će postaviti jasan i definiran okvir zadržavanja podataka elektroničke komunikacije. Vijeće Europske unije za pravosuđe i unutarnje poslove donijelo je 19. prosinca 2002. Zaključke u kojima se naglašava važnost podataka koji se odnose na uporabu elektroničkih komunikacija kao vrijedna sredstva u sprječavanju, istrazi, otkrivanju i progonu kaznenih djela, posebno organiziranog kriminala.[17] Deklaracijom o borbi protiv terorizma, koju je donijelo 25. ožujka 2004. godine, Europsko vijeće uputilo je Vijeće EU-a da ispita mjere za utvrđivanje pravila pružatelja usluga o zadržavanju podataka o komunikacijskom prometu, dok je Deklaracijom od 13. srpnja 2005. godine Vijeće EU-a osudilo terorističke napade i potvrdilo potrebu za što skorijim donošenjem zajedničkih mjera vezanih uz zadržavanje telekomunikacijskih podataka.

Sve navedeno, kao i želja za harmonizacijom odredaba o zadržavanju podataka elektroničke komunikacije, s obzirom na uočene znatne razlike među nacionalnim odredbama o zadržavanju podataka u skladu s prijašnjom Direktivom 2002/58/EZ rezultiralo je prihvaćanjem Direktive o zadržavanju podataka 2006. godine.[18] U odnosu na predmet i polje primjene cilj je Direktive uskladiti odredbe država članica koje se odnose na obveze pružatelja usluga u odnosu na zadržavanje određenih podataka koje skupljaju ili obrađuju pružatelji da bi se osiguralo da ti podatci budu dostupni zbog istrage, otkrivanja i progona teških kaznenih djela. Dakle, svrha zadržavanja podataka ograničena je u smislu kaznenih djela tako da nije svako kazne-

[15] Riječ je o odredbi koja će poslije biti predmet tumačenja presude *Tele2* Suda EU-a iz prosinca 2016. godine.

[16] *Turkalj*, 2002, 10, 1–15.

[17] *2477th Council meeting – JUSTICE AND HOME AFFAIRS – Brussels, 19 December 2002; Council Conclusions on Information technologies and the investigation and prosecution of organised crime, doc. 15691/02*

[18] Više u *Blakeney*, 2007, 1–5; *Lynskey*, 2014, 1790–1791; *Tracol*, 2014, 737–738.

no djelo relevantno. Direktiva jasno definira kriterije za zadržavanje podataka od pružatelja usluga te za pristup nadležnih tijela tim podatcima kao i potrebna jamstva zaštite osobnih podataka i sigurnosti zadržanih podataka. Direktiva propisuje obvezu pružatelja usluga da prikupljaju podatke o prometu i lokaciji kao i podatke vezane za prepoznavanje pretplatnika ili korisnika te traži da se osigura dostupnost tih podataka radi prevencije, istrage, otkrivanja i progona teških (ozbiljnih) kaznenih djela, posebice organiziranog kriminala i terorizma, s time da se pojam i okolnost teških kaznenih djela ostavlja na utvrđivanje državama u skladu s unutarnjim pravom.[19] Podatci koji se moraju zadržavati uključuju podatke o prometu i lokaciji pravnih i fizičkih osoba te vezane podatke nužne za identificiranje pretplatnika ili registriranog korisnika.[20] Ne smiju se pohranjivati podatci koji otkrivaju sadržaj komunikacije, dok se razdoblje zadržavanja podataka propisuje kao ne kraće od šest mjeseci niti dulje od dvije godine.[21] Osim samog zadržavanja podataka Direktiva regulira i pristup tim podatcima, odnosno nameće državama članicama obvezu donošenja mjera da bi osigurale da se pristup zadržanim podatcima omogućuje samo nadležnim nacionalnim tijelima u posebnim slučajevima u skladu s nacionalnim pravom te u skladu sa zahtjevima nužnosti i proporcionalnosti.[22] Konačno, Direktiva posebno propisuje potrebna minimalna sigurnosna načela (jamstva) koja pružatelji usluga moraju osigurati kao i provoditi tehničke i organizacijske mjere da bi se zadržani podatci zaštitili od slučajna ili nezakonita uništenja, slučajna gubitka ili izmjene, ili od neovlaštena ili nezakonita pohranjivanja, obrade, pristupa ili otkrivanja. Uz navedene mjere važna je obveza država da osiguraju neovisan nadzor nad provedbom odgovarajućih domaćih odredaba.[23]

Odmah nakon stupanja na snagu, kao još i tijekom pregovora[24], Direktiva je podvrgnuta ozbiljnim kritikama nevladinih udruga[25], pružatelja usluga i Europskog nadzornika za zaštitu osobnih podataka[26], kao „bez sumnje najinvazivniji instrument u području privatnosti građana EU-a s obzirom na opseg zadiranja i broj obuhvaćenih osoba".[27] Direktivu je ozbiljno kritizirala i radna skupina iz članka 29.[28] Takvo raširе-

[19] Vidi više *Vaciago*, 2014, 66; *Galli*, 2016, 467–468; *Stoeva*, 2014, 583.

[20] Vidi čl. 5., st. 1.; *op. cit.*, 54–63.

[21] Vidi čl. 5., st. 2. i čl. 6.; *op. cit.*, 54–63.

[22] Vidi čl. 4.; *op. cit.*, 54–63.

[23] Vidi čl. 7. i čl. 9.; *op. cit.*, 54–63.

[24] Vidi više *Galli*, 2016, 466–469.

[25] Vidi više *Lynskey*, 2014, 1792.

[26] Vidi više *Munir*; *Yasin*; *Bakar*, 2017, 73.

[27] O tome govori Drewry nazivajući navedenu direktivu najtežim zadiranjem u ljudska prava, vidi *Drewry*, 2016, 733.

[28] Radna skupina osnovana je na temelju članka 29. Direktive 95/46/EZ. Ona je neovisno europsko savjetodavno tijelo za zaštitu podataka i privatnosti. Njezine su zadaće opisane u članku 30. Direktive 95/46/EZ i članku 15. Direktive 2002/58/EZ. Više o kritikama radne skupine *Tracol*, 2014, 739; *Munir*; *Yasin*; *Bakar*, 2017, 72.

no nezadovoljstvo rezultiralo je tužbama kojima civilne organizacije (*Digital Rights Ireland*), fizičke i pravne osobe (*Tele2*) na nacionalnim sudovima postavljaju pitanje zakonitosti mjera zadržavanja podataka. U povodu tih tužbi, a zbog zahtjeva za prethodnu odluku nacionalnih sudova, Sud Europske unije donio je odluke kojima postavlja granice postojećem režimu zadržavanja podataka.

5. PRAVNI OKVIR ZADRŽAVANJA PODATAKA U REPUBLICI HRVATSKOJ

Pitanje zadržavanja podataka elektroničke komunikacije i pristupa nadležnih tijela tim podatcima u pravnom poretku RH regulirano je nizom propisa. Posebice se ističu Zakon o elektroničkim komunikacijama (dalje u tekstu: ZEK)[29], Zakon o kaznenom postupku (dalje u tekstu: ZKP)[30] te Zakon o sigurnosno-obavještajnom sustavu Republike Hrvatske (dalje u tekstu: ZSOS).[31] Osim toga, važni su još i Zakon o obrani[32], Pravilnik o vojnopolicijskim poslovima i provedbi ovlasti ovlaštenih službenih osoba vojne policije[33] te Uredba o obvezama iz područja nacionalne sigurnosti Republike Hrvatske za pravne i fizičke osobe u telekomunikacijama (dalje u tekstu: Uredba).[34] Navedenim propisima uređuje se niz pitanja važnih za zadržavanje podataka poput razdoblja zadržavanja, kruga osoba obuhvaćenih zadržavanjem podataka, kategorija podataka te sredstava komunikacije, pristupa nadležnih tijela tim podatcima i jamstava zaštite tih podataka.

U odnosu na svrhu zadržavanja podataka čl. 109. ZEK-a propisuje obvezu pružatelja usluga za zadržavanje podataka o elektroničkim komunikacijama radi omogućivanja provedbe istrage, otkrivanja i kaznenog progona kaznenih djela te radi zaštite obrane i nacionalne sigurnosti u skladu s posebnim zakonima. Takvom formulacijom zakonske norme zadržavanje podataka vezuje se uz počinjenje kaznenog djela, pri čemu se težina kaznenog djela vezuje uz njegovo određenje u posebnim propisima. Poseban propis koji određuje kaznena djela za koja je moguć pristup zadržanim podatcima jest ZKP. Čl. 339.a ZKP-a propisuje da se dokazna radnja, koja se sastoji u pristupu zadržanim podatcima, može provesti samo radi prikupljanja dokaza za kaznena djela za koja je moguće odrediti posebne dokazne radnje te druga kaznena

[29] Zakon o elektroničkim komunikacijama, NN, br. 73/08, 90/11, 133/12, 80/13, 71/14.

[30] Zakon o kaznenom postupku, NN, br. 152/08, 76/09, 80/11, 121/11, 91/12, 143/12, 56/13, 145/13, 152/14, 70/17.

[31] Zakon o sigurnosno-obavještajnom sustavu Republike Hrvatske, NN, br. 79/06, 105/06.

[32] Zakon o obrani, NN, br. 73/13, 75/15, 27/16.

[33] Pravilnik o vojnopolicijskim poslovima i provedbi ovlasti ovlaštenih službenih osoba vojne policije, NN, br. 44/14.

[34] Uredba o obvezama iz područja nacionalne sigurnosti Republike Hrvatske za pravne i fizičke osobe u telekomunikacijama, NN, br. 64/08, 76/13.

djela za koja je propisana kazna zatvora teža od pet godina.[35] Time je ujedno sužena svrha zadržavanja, ali i pristupa podatcima samo na one koji su potrebni za otkrivanje i procesuiranje najtežih kaznenih djela.

Pravni okvir kojim su propisane vrste podataka na koje se odnosi obveza zadržavanja podataka sadržan je u ZEK-u, ZKP-u, ZSOS-u i Uredbi. Odredbom čl. 110. ZEK-a propisane su i vrste podataka na koje se odnosi obveza zadržavanja podataka, a to su: podatci potrebni za praćenje i utvrđivanje izvora komunikacije; podatci potrebni za utvrđivanje odredišta komunikacije; podatci potrebni za utvrđivanje nadnevka, vremena i trajanja komunikacije; podatci potrebni za utvrđivanje vrste komunikacije; podatci potrebni za utvrđivanje korisničke komunikacijske opreme ili opreme; podatci potrebni za utvrđivanje lokacije pokretne komunikacijske opreme. Zadržani podatci obuhvaćaju i podatke koji se odnose na neuspješne pozive. Odredba čl. 105., st. 4. ZEK-a propisuje da utvrđene podatke o zlonamjernim ili uznemirujućim pozivima, SMS ili MMS porukama operator javnih komunikacijskih usluga mora zadržati u skladu s čl. 109. i bez odgode dostaviti nadležnoj policijskoj upravi na daljnje postupanje. Posebice treba istaknuti da Zakon zabranjuje zadržavanje podataka koji otkrivaju sadržaj komunikacije. Ujedno su propisane i prekršajne sankcije u slučaju neispunjavanja relevantnih obveza operatora, što se smatra teškom povredom ZEK-a.

ZKP također govori o vrstama podataka koji se zadržavaju kada propisuje uvjete pristupa zadržanim podatcima. Tako članak 339.a ZKP-a propisuje da policija na temelju naloga suca istrage može od operatora javnih komunikacijskih usluga zatražiti za registriranog vlasnika ili korisnika telekomunikacijskog sredstva, ako postoji sumnja da je upravo on počinio kazneno djelo, 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.

U domaćemu pravnom okviru također je na snazi prije uvedena mjera obveznoga preventivnog zadržavanja podataka građana (dakle neovisno o Direktivi) u skladu sa ZSOS-om iz 2006. godine i na temelju njega prihvaćene Uredbe. Odredba čl. 21. Uredbe propisuje da su pravne i fizičke osobe koje raspolažu javnom telekomunikacijskom mrežom i pružaju javne telekomunikacijske usluge i usluge pristupa u RH dužne pohraniti sljedeće kategorije podataka potrebnih za otkrivanje i identificiranje izvora komunikacije: u slučaju fiksne i mobilne telefonije broj s kojeg je inicirana komunikacija; ime/prezime, naziv pravne osobe i adresa pretplatnika ili registriranog korisnika, a u slučaju internetskog pristupa: e-pošte, internetske telefonije i drugih oblika podatkovne komunikacije.[36] Formulaciju „i druge oblike podatkovne

[35] Vidi ZKP, NN, br. 152/08, 76/09, 80/11, 121/11, 91/12, 143/12, 56/13, 145/13, 152/14, 70/17.

[36] Vidi članak 21. Uredbe.

komunikacije" moglo bi se tumačiti da obuhvaća i sam sadržaj komunikacije. Ako bi to bio slučaj, to bi bilo u suprotnosti s obvezama iz Direktive kojima se zabranjuje zadržavanje sadržaja komunikacije.

Krug osoba koje su obuhvaćene zadržavanjem podataka definiran je ZEK-om i ZSOS-om. Formulacija iz članka 109. ZEK-a govori općenito o obvezi zadržavanja podataka bez specificiranja kruga osoba. Težište se stavlja na zadržavanje podataka, pri čemu se implicitno misli na podatke svih korisnika elektroničkih komunikacija. Za razliku od toga, ZSOS propisuje čuvanje podataka o ostvarenu telekomunikacijskom prometu koji se odnose na korisnike usluga.[37] Iz te odredbe proizlazi da se čuvanje podataka odnosi na sve korisnike elektroničke komunikacije. Dakle, takvim uređenjem kruga osoba na općenit i neselektivan način obuhvaća se sve pretplatnike i registrirane korisnike elektroničkih komunikacija bez obzira na to postoji li za njih bilo kakva naznaka koja bi navela na mišljenje da njihovo ponašanje može imati veze s teškim kaznenim djelima te se odnosi na sva sredstva elektroničke komunikacije kao i na sve podatke o prometu.

U odnosu na razdoblje zadržavanja podataka prema čl. 109. ZEK-a pružatelji usluga obvezni su zadržati podatke dvanaest mjeseci od dana obavljene komunikacije. U skladu s odredbom čl. 19., st. 5. ZSOS-a podatci o ostvarenu telekomunikacijskom prometu koji se odnose na korisnike usluga čuvaju se godinu dana. Tu se postavlja pitanje je li to razdoblje stvarno nužno za ostvarivanje legitimnih ciljeva poput progona teških kaznenih djela ili bi se ista svrha mogla ostvariti i zadržavanjem podataka u kraćem razdoblju.

U odnosu na pristup nadležnih tijela zadržanim podatcima od strane ovlaštenih tijela relevantne odredbe sadržavaju ZEK i ZKP. Odredba čl. 109., st. 4. ZEK-a propisuje da operatori javnih komunikacijskih mreža i javno dostupnih elektroničkih komunikacijskih usluga provode obvezu zadržavanja podataka tako da se zadržani podatci mogu bez odgode dostaviti nadležnom tijelu – Operativno-tehničkom centru za nadzor telekomunikacija (OTC).

Do 2002. godine policija je svoje zahtjeve prema davateljima telekomunikacijskih usluga temeljila na odredbi čl. 177., st. 2. ZKP-a (NN, br. 110/97, 27/98, 58/99 i 112/99) koja je određivala poduzimanje i „druge potrebne mjere i radnje" radi djelotvorne provedbe izvida kaznenih djela za koja se progoni po službenoj dužnosti. Novelom ZKP-a 2002. godine izrijekom je kao ovlast policije u provedbi izvida kaznenih djela propisano i utvrđivanje istovjetnosti telekomunikacijskih adresa koje su u određe-

[37] Članak 19., st. 5. ZSOS-a propisuje da su pravne i fizičke osobe koje raspolažu javnom telekomunikacijskom mrežom i pružaju javne telekomunikacijske usluge i usluge pristupa u Republici Hrvatskoj dužne čuvati podatke o ostvarenu telekomunikacijskom prometu koji se odnose na korisnike usluga godinu dana.

nom razdoblju uspostavile vezu. Zakon o policijskim poslovima i ovlastima propisivao je da policija na temelju pisana odobrenja načelnika Uprave kriminalističke policije ili načelnika Policijskoga nacionalnog ureda za suzbijanje korupcije i organiziranog kriminaliteta ili načelnika policijske uprave može zatražiti od davatelja komunikacijskih usluga provjeru istovjetnosti, trajanja i učestalosti komunikacije s određenim elektroničkim komunikacijskim adresama ako je to potrebno 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.

U listopadu 2013. godine dopunom odredbe čl. 339.a ZKP-a (NN, br. 145/13), kojim se provjera uspostavljanja elektroničkoga komunikacijskog kontakta regulira ZKP-om kao dokazna radnja, napravljen je bitan korak u zaštiti privatnosti vlasnika ili korisnika komunikacijskih uređaja. Kao što je prethodno izloženo, prema dotadašnjemu pravnom uređenju bila je riječ o izvidnoj radnji policijskih tijela. S obzirom na stupanj zahvata u temeljna ljudska prava, koji je znatno viši nego što je to slučaj kod ostalih izvidnih radnji, provjeru uspostavljanja telekomunikacijskog kontakta radi prikupljanja dokaza i otkrivanja počinitelja kaznenih djela za koja se kazneni postupak pokreće po službenoj dužnosti zakonodavac je odlučio urediti u ZKP-u uz jamstvo višeg stupnja zaštite temeljnih prava registriranih vlasnika ili korisnika uređaja, osobito prava na privatnost.

Dodatna zaštita odnosno sigurnost osigurana je novelom odredbe čl. 339.a ZKP-a iz 2014. godine[38] kojom je dodatno sužena mogućnost provođenja dokazne radnje provjere uspostavljanja telekomunikacijskog kontakta i to tako da se ta dokazna radnja može provesti samo radi prikupljanja dokaza za kaznena djela za koja je moguće odrediti posebne dokazne radnje te druga kaznena djela za koja je propisana kazna zatvora teža od pet godina, a ne više za sva kaznena djela za koja se kazneni postupak pokreće po službenoj dužnosti. Naime, imajući u vidu opseg zadiranja te dokazne radnje u privatnost osobe prema kojoj se ona provodi, bilo je potrebno ograničiti mogućnost pristupa tim podatcima i njihovu naknadnu uporabu samo na teška kaznena djela kod kojih se takvo zadiranje može opravdati. Navedeno je u skladu s odredbama čl. 7. i 8. Povelje o temeljnim pravima Europske unije koji postavljaju više zaštitnih mehanizama kojima se osigurava poštivanje privatnog života i zaštita osobnih podataka pojedinaca u slučaju zadržavanja podataka, između ostaloga i zaštitni mehanizam koji nalaže da pristup i uporaba zadržanih podataka moraju biti ograničeni, što se novelom ZKP-a i osigurava.

Odredba čl. 339.a ZKP-a propisuje da policija na temelju naloga suca istrage može od operatora javnih komunikacijskih usluga zatražiti provjeru registriranog vlasnika ili korisnika telekomunikacijskog sredstva ako postoji sumnja da je upravo on počinio

[38] Vidi ZKP, NN, br. 152/14.

kazneno djelo u odnosu na istovjetnost, trajanje i učestalost 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. Ista se provjera može naložiti i za osobu povezanu s osobom za koju postoji sumnja da je počinitelj takva kaznenog djela. Nalog za provjeru uspostavljanja telekomunikacijskog kontakta sudac istrage izdaje na temelju obrazložena prijedloga nadležna državnog odvjetnika.

ZKP postavlja jasan i objektivan kriterij o tome za koja se kaznena djela može ostvariti pristup zadržanim podatcima. ZKP osigurava jamstvo sudske kontrole pristupa zadržanim podatcima kao i korištenje tim podatcima samo u zakonom propisanim svrhama. Istodobno je jasno propisano da se podatci pribavljeni bez odgovarajućeg naloga suca istrage ne mogu upotrijebiti kao dokaz u postupku. Također, odredbama ZKP-a omogućeno je informiranje osoba čiji su podatci zadržani jer članci 183., 184. i 184.a ZKP-a propisuju pravo okrivljenika na uvid u spis.

U pogledu zaštitnih jamstava sigurnosti i zaštite zadržanih podataka odredba čl. 109., st. 5. ZEK-a posebno propisuje načela sigurnosti zadržanih podataka kojih su se pružatelji usluga obvezni pridržavati: zadržani podatci moraju biti prikladno zaštićeni od slučajna ili nezakonita uništenja, slučajna gubitka ili izmjene, neovlaštene ili nezakonite pohrane, obrade, pristupa ili razotkrivanja; pristup zadržanim podatcima mora se ograničiti isključivo na ovlaštene osobe nadležnih tijela koji imaju pravo na pristup tim podatcima; zadržani podatci moraju se uništiti nakon isteka razdoblja zadržavanja uz iznimke; pružatelji usluga moraju o vlastitom trošku osigurati sve potrebne tehničke i ustrojstvene mjere radi pune primjene načela sigurnosti. U skladu s odredbama Direktive 2002/58 pružatelji usluga obvezni su poduzeti prikladne tehničke i organizacijske mjere koje osiguravaju učinkovitu zaštitu zadržanih podataka od rizika zlouporabe kao i od svakoga nezakonita pristupa tim podatcima. Pružatelji usluga moraju prikladnim tehničkim i organizacijskim mjerama radi osiguranja puna integriteta i povjerljivosti navedenih podataka jamčiti osobito visoku razinu zaštite i sigurnosti.

Da bi se osiguralo poštivanje pravila o zadržavanju podataka, zakonodavac je odredio i prekršajnu odgovornost pružatelja usluga. Operateri mogu biti prekršajno kažnjeni prema odredbi čl. 118. ZEK-a ako ne ispunjavaju svoje obveze zadržavanja podataka elektroničke komunikacije.

6. PRESUDE SUDA EUROPSKE UNIJE O ZADRŽAVANJU PODATAKA

Nakon terorističkih napada na SAD, Veliku Britaniju i Španjolsku težište europskih politika usmjerava se na jačanje sigurnosti uz zanemarivanje temeljnih prava i sloboda. Narušava se ravnoteža između zahtjeva za poštivanje ljudskih prava i potreba

sigurnosti. Narušena ravnoteža počela se postupno vraćati stavljanjem sve većeg fokusa na zaštitu ljudskih prava. Sud Europske unije svojim je presudama bio važan korektiv mjera koje su se donosile radi borbe protiv terorizma na području Europske unije. Sud Europske unije do sada je donio nekoliko presuda koje su od izravna utjecaja na zaštitu ljudskih prava u provedbi antiterorističke politike Europske unije. Ponajprije je riječ o presudama donesenim u povodu određenih restriktivnih mjera protiv pojedinaca i entiteta zbog njihove uključenosti u financiranje terorizma. Vjerojatno je najpoznatija presuda Velikog vijeća u predmetu *Kadi* iz 2008. godine u kojoj je Sud ustanovio povredu prava vlasništva u odnosu na Kadija.[39] Slijedeći zaključke do kojih je došao Sud u predmetu *Kadi*, Sud je i u predmetu *Hassan* preinačio prvostupanjsku presudu te ukinuo Uredbu (EZ) 881/2002 u odnosu na *Hassana i Ayadija*.[40] Sud je utvrdio da pravo obrane kao i pravo na učinkovitu sudsku zaštitu nisu bili poštivani u tim predmetima.[41] Također je ustanovio povredu prava vlasništva primjenom mjera zamrzavanja imovine kao neopravdane restrikcije prava vlasništva.[42] Takvu razvoju odnosa pridonijele su i dvije presude Suda EU-a koje se odnose na zadržavanje podataka, a imaju presudno značenje za buduće pravno uređenje zadržavanja podataka na europskoj i na nacionalnoj razini. Riječ je o presudama *Digital Rights* iz 2014. godine i *Tele2* iz 2016. godine.

Presudom *Digital Rights* Sud je stavio izvan snage Direktivu 2006/24/EZ o zadržavanju podataka. Povod presudi bili su zahtjevi za prethodnu odluku koje su postavili austrijski[43] i irski nacionalni sud.[44] Zahtjev koji je u lipnju 2012. godine uputio irski sud odnosio se na zakonitost nacionalnih zakonodavnih i upravnih mjera koje se odnose na zadržavanje podataka u vezi s elektroničkim komunikacijama, dok se zahtjev koji je u prosincu 2010. godine uputio austrijski sud odnosio na ustavne tužbe u vezi s usklađenošću zakona kojim se Direktiva 2006/24 prenosi u domaće austrijsko pravo s federalnim ustavnim zakonom.

Konkretno, oba zahtjeva za prethodnu odluku odnose se na pitanje usklađenosti Direktive 2006/24 o zadržavanju podataka s pravom na poštivanje privatnog života

[39] Presuda Velikog vijeća od 3. rujna 2008. u spojenim predmetima C-402/05 P i C-415/05 P, *Yassin Abdullah Kadi i Al Barakaat International Fundation protiv Vijeća Europske unije* uz potporu Španjolske, Francuske, Nizozemske i Europske komisije, *European Court Reports*, 2008., 1-06351.

[40] Presuda Suda od 3. prosinca 2009. u predmetima C-399/06 P i C-403/06 P, *Hassan protiv Vijeća Europske unije i Europske komisije* te *Ayadi protiv Vijeća Europske unije, European Court Reports*, 2009.

[41] *Ibid.*, §§ 84–86.

[42] *Ibid.*, § 93.

[43] Detaljno u C-594/12 *Request for a preliminary ruling from the Verfassungsgerichtshof (Austria) lodged on 19 December 2012 – Kärntner Landesregierung and Others*, OJ C 79, 16. ožujka 2013.

[44] 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.

i komuniciranja iz članka 7. Povelje Europske unije o temeljnim pravima kao i s pravom na zaštitu osobnih podataka iz članka 8. Povelje te s pravom na slobodu izražavanja iz članka 11. Povelje, odnosno je li Direktiva 2006/24 usklađena s Poveljom s obzirom na to da omogućuje pohranjivanje velike količine vrsta podataka u odnosu na neograničen broj osoba tijekom dugog razdoblja, a zadržavanje se odnosi gotovo isključivo na osobe čije ponašanje nikako ne opravdava zadržavanje podataka koji se na njih odnose.

Kako navodi u obrazloženju presude, Sud Europske unije smatra da Direktiva 2006/24 o zadržavanju podataka ne određuje jasna i precizna pravila koja bi uredila doseg miješanja u temeljna prava iz članaka 7. i 8. Povelje, odnosno da to miješanje nije precizno ograničeno odredbama koje bi jamčile da je stvarno ograničeno na ono što je strogo nužno. Također, Sud smatra da Direktiva ne propisuje jasne kriterije pristupa tim podatcima te da ne određuje dostatna jamstva zaštite osobnih podataka i sigurnosti zadržanih podataka.[45]

Sud smatra da se miješanje u pravo na poštivanje privatnog života i komuniciranja očituje u činjenici da tako zadržani podatci omogućuju saznanje s kojom je osobom pretplatnik ili registrirani korisnik komunicirao i kojim sredstvom kao i utvrđivanje vremena komunikacije te mjesta s kojeg se ona odvijala, odnosno omogućuju uvid u učestalost komunikacija pretplatnika ili registriranog korisnika s određenim osobama tijekom danog razdoblja. Ti podatci, uzeti zajedno, mogu omogućiti donošenje vrlo preciznih zaključaka o privatnom životu osoba čiji su podatci zadržani kao što su svakodnevne navike, mjesta trajnih ili privremenih boravaka, dnevna ili druga kretanja, obavljane aktivnosti, društveni odnosi i društvene sredine koje su te osobe posjećivale.[46] Pristup nadležnih tijela tim podatcima dodatno je miješanje u to temeljno pravo. Navedeno posljedično dovodi i do miješanja u pravo na slobodu izražavanja zajamčeno člankom 11. Povelje jer takvo zadržavanje podataka može imati utjecaj na korisničko korištenje komunikacijskom mrežom, odnosno na njihovo uživanje slobode izražavanja.[47] Konačno, miješanje u pravo na zaštitu osobnih podataka manifestira se kroz činjenicu da je takvo zadržavanje podataka obrada osobnih podataka.

U odnosu na opravdanje miješanja u ta temeljna prava Sud smatra da je svako ograničenje prava i sloboda moguće samo ako je potrebno i ako zaista odgovara ciljevima od općeg interesa koje priznaje Unija ili potrebi zaštite prava i sloboda drugih osoba.[48] Sud je svjestan da se zadržavanjem podataka ne dopušta uvid u sadržaj elektroničke komunikacije, nego samo na podatke o prometu i lokaciji te da pruža-

[45] Vidi toč. 65 presude.
[46] Vidi toč. 26 i 27 presude.
[47] Vidi toč. 28 presude.
[48] Vidi toč. 38 presude.

telji usluga moraju poštovati načela zaštite i sigurnosti podataka. Ipak Sud, ne osporavajući da je borba protiv teškog kriminala, a osobito borba protiv organiziranog kriminala i terorizma od primarne važnosti za jamstvo javne sigurnosti[49], smatra da takav cilj koji je u općem interesu ne može opravdati da se mjera zadržavanja, kao što je ona uspostavljena Direktivom o zadržavanju podataka, smatra nužnom u svrhu navedene borbe. Sud smatra da navedena Direktiva na općenit način obuhvaća svaku osobu i sva sredstva elektroničke komunikacije kao i sve podatke o prometu bez ikakva razlikovanja, ograničenja ili iznimke s obzirom na cilj borbe protiv teških kaznenih djela. Direktiva se odnosi općenito na sve osobe koje se koriste uslugama elektroničkih komunikacija a da se pritom osobe čiji se podatci zadržavaju ne nalaze, čak ni posredno, u situaciji koja može dovesti do kaznenih progona. Ona se dakle primjenjuje i na osobe za koje ne postoji nikakva naznaka koja bi navela na mišljenje da njihovo ponašanje može imati vezu, čak i posrednu ili daleku, s teškim kaznenim djelima te nije ograničena na zadržavanje podataka iz privremenog razdoblja, i/ili određena zemljopisnog područja, i/ili dana kruga osoba koje mogu kako biti umiješane u teško kazneno djelo ili na osobe koje, ako se zadrže njihovi podatci, mogu zbog drugih razloga pridonijeti sprječavanju, otkrivanju ili progonu teških kaznenih djela.[50]

Što se tiče samog pristupa zadržanim podatcima, prema mišljenju Suda, Direktiva ne određuje nikakav objektivan kriterij koji bi omogućio ograničenje pristupa nadležnih nacionalnih tijela podatcima i njihove naknadne uporabe radi sprječavanja, otkrivanja ili kaznenih progona. Također, Direktiva ne propisuje da pristup i naknadno korištenje podatcima moraju biti strogo ograničeni sa svrhom sprječavanja i otkrivanja teških kaznenih djela, nego samo navodi da svaka država članica propisuje postupak i uvjete koji se moraju ispuniti da bi se ostvario pristup zadržanim podacima u skladu sa zahtjevima nužnosti i proporcionalnosti.[51] Kritika ide i u smjeru da pristup nadležnih nacionalnih tijela zadržanim podatcima nije podređen prethodnom nadzoru suda ili neovisnoga upravnog tijela čija bi odluka ograničavala pristup podatcima samo na ono što je strogo nužno te korištenje njima. Konačno, u odnosu na trajanje zadržavanja, koje je utvrđeno između najmanje šest mjeseci i najviše 24 mjeseca, nije pobliže određeno da utvrđivanje trajanja zadržavanja mora biti utemeljeno na objektivnim kriterijima da bi se zajamčilo da je ograničeno na ono što je strogo nužno.[52]

Zbog proglašenja Direktive o zadržavanju podataka nevaljanom na razini Europske unije više ne postoji zakonski okvir koji regulira područje zadržavanja podataka

[49] Vidi toč. 51 presude.
[50] Vidi toč. 57 i 58 presude.
[51] Vidi toč. 61 i 62 presude.
[52] Vidi toč. 63 presude.

elektroničke komunikacije. Budući da su nacionalna zakonodavstva koja uređuju to područje i dalje bila na snazi (što nepromijenjena, što modificirana u skladu s praksom Suda EU-a), postavilo se pitanje usklađenosti takvih nacionalnih rješenja u odnosu na propise EU-a koji su ostali na snazi.

Nakon presude *Digital Rights* u Švedskoj je *Tele2 Sverige* odlučio uskladiti svoje postupanje sa zahtjevima iz same presude te je obavijestilo nadležna nacionalna tijela da će prestati zadržavati podatke koji se odnose na elektroničke komunikacije i da će ukloniti dotadašnje zadržane podatke. Poseban izvjestitelj švedskog ministra pravosuđa analizirao je pozitivne propise o zadržavanju podataka te je dao mišljenje da se oni ne protive ni pravu Unije ni Europskoj konvenciji za zaštitu ljudskih prava i temeljnih sloboda, odnosno da presudu *Digital Rights* nije moguće tumačiti tako da je njome ograničeno samo načelo općeg i neselektivnog zadržavanja podataka.[53] Na temelju takva mišljenja nadležna tijela zatražila su od *Tele2* da zadrži te podatke. Smatrajući da se nalaz posebnog izvjestitelja temelji na pogrešnu tumačenju presude *Digital Rights* te da se obveza zadržavanja podataka protivi temeljnim pravima zajamčenima Poveljom, *Tele2 Sverige* podnio je tužbu protiv naloga za zadržavanjem podataka. U okviru navedenog postupka švedski sud postavlja zahtjev za prethodnim pitanjem u smislu treba li članak 15., stavak 1. Direktive 2002/58 u vezi s člancima 7. i 8. te člankom 52., stavkom 1. Povelje tumačiti tako da mu se protivi nacionalni propis kojim se radi borbe protiv kriminaliteta određuje opće i neselektivno zadržavanje svih podataka o prometu i lokaciji svih pretplatnika i registriranih korisnika u vezi sa svim sredstvima elektroničke komunikacije.[54]

Drugi zahtjev Sudu EU-a za prethodnim pitanjem, koji je u prosincu 2015. godine uputio drugostupanjski (žalbeni) engleski sud, rezultat je zahtjeva pojedinih fizičkih osoba za nadzorom zakonitosti, odnosno usklađenosti nacionalnog propisa o zadržavanju podataka s pravom Unije. Naime, prema mišljenju prvostupanjskog suda, budući da je Sud EU-a utvrdio da Direktiva 2006/24 nije u skladu s načelom proporcionalnosti, nacionalni propis čiji je sadržaj istovjetan njezinu sadržaju također ne može biti u skladu s tim načelom. Ministar unutarnjih poslova podnio je žalbu na tu presudu te je žalbeni sud podnio zahtjev za prethodnom odlukom u smislu pitanja uspostavlja li presuda *Digital Rights* važne zahtjeve prava Unije primjenjive na nacionalni sustav države članice koji uređuje pristup podatcima zadržanima u skladu s

[53] Poseban izvjestitelj švedskog ministra pravosuđa smatra da se presuda *Digital Rights* nije smjela tumačiti tako da je Sud u njoj utvrdio niz kriterija koji bi redom morali biti zadovoljeni da bi se neki propis mogao smatrati proporcionalnim. Valja ocijeniti sve okolnosti da bi se utvrdila sukladnost švedskog propisa s pravom Unije poput opsega zadržavanja podataka s obzirom na odredbe o pristupu podacima, trajanju njihova zadržavanja te zaštiti i sigurnosti tih podataka.

[54] Detaljnije vidi u C-203/15: *Request for a preliminary ruling from the Kammarrätten i Stockholm (Sweden)*, OJ C 221, 6. svibnja 2015.

nacionalnim zakonodavstvom radi usklađivanja s člancima 7. i 8. Povelje? Proširuje li presuda *Digital Rights* doseg članaka 7. i/ili 8. Povelje u odnosu na doseg članka 8. EKLJP-a kako je utvrđen sudskom praksom Europskog suda za ljudska prava? Sud EU-a to je pitanje ocijenio nedopuštenim navodeći da ono ne može utjecati na tumačenje Direktive 2002/58, odnosno da odgovor na to pitanje ne može pružiti elemente za tumačenje prava Unije.

Konačno, u prosincu 2016. godine Sud EU-a donio je presudu *Tele2* kojom daje mišljenje o usklađenosti nacionalnih propisa o zadržavanju podataka s odredbom čl. 15., st. 1. Direktive 2002/58/EZ o privatnosti i elektroničkim komunikacijama. Kako navodi u obrazloženju presude, Sud Europske unije smatra da je nacionalni propis koji u cilju borbe protiv kriminaliteta određuje opće i neselektivno zadržavanje svih podataka o prometu i lokaciji svih pretplatnika i registriranih korisnika u smislu svih sredstava elektroničke komunikacije u suprotnosti s odredbom čl. 15., st. 1. Direktive 2002/58/EZ o privatnosti i elektroničkim komunikacijama kao i nacionalni propis kojim se uređuje zaštita i sigurnost podataka o prometu i lokaciji i, osobito, pristup nadležnih nacionalnih tijela zadržanim podatcima kad svrha tog pristupa u okviru borbe protiv kriminaliteta nije ograničena na borbu protiv teških kaznenih djela, kad se navedeni pristup ne podvrgava prethodnom nadzoru suda ili neovisnoga upravnog tijela i kad nije propisano da se predmetni podatci zadržavaju na području Unije.[55]

Sud Europske unije navodi da je, između ostalog, cilj Direktive poštivanje prava određenih u čl. 7. i 8. Povelje te da je očito da je zakonodavac Unije želio postići to da visoka razina zaštite osobnih podataka i privatnog života bude i dalje zajamčena za sve elektroničke komunikacijske usluge, bez obzira na primijenjenu tehnologiju. Upravo zato Direktiva 2002/58 sadržava posebne odredbe kojima je cilj zaštititi korisnike elektroničkih komunikacijskih usluga od opasnosti za osobne podatke i privatni život koje su rezultat novih tehnologija i veće sposobnosti automatskog pohranjivanja i obrade podataka.[56]

Sud priznaje da odredba čl. 15., st. 1. Direktive omogućuje državama članicama da uvedu iznimke od obveze država članica da građanima EU-a jamče povjerljivost komunikacija, a time i njihovih osobnih podataka, ali Sud smatra da postojanje režima općeg i neselektivnog zadržavanja svih podataka o prometu i lokaciji svih pretplatnika i registriranih korisnika u smislu svih sredstava elektroničke komunikacije, koje se provodi sustavno i stalno, postaje pravilo, a ne iznimka kako to zahtijeva Direktiva.[57] Takvo zadržavanje podataka ne određuje nikakvo razlikovanje, ograničenje ili iznimku s obzirom na cilj koji se želi postići. Ono se općenito odnosi na sve

[55] Vidi izreku presude, toč. 1 i 2.
[56] Vidi toč. 82 presude.
[57] Vidi toč. 88 i 89 presude.

osobe koje se koriste elektroničkim komunikacijskim uslugama a da se pritom te osobe ne nalaze, čak ni posredno, u situaciji koja može dovesti do kaznenih progona. Takvo zadržavanje prelazi granice strogo nužnog i ne može se smatrati opravdanim u demokratskom društvu. Sud podsjeća da sama odredba čl. 15., st. 1. Direktive propisuje da je mjera kojom se odstupa od načela povjerljivosti komunikacija i s njima povezanih podataka o prometu dopuštena samo ako je to nužna, prikladna i razmjerna mjera unutar demokratskog društva, odnosno da ta mjera mora biti strogo razmjerna svrsi za koju se poduzima. Također, ista odredba zahtijeva da se zadržavanje podataka provodi tijekom ograničenog razdoblja i dok je opravdano nekim od propisanih ciljeva (zaštita nacionalne sigurnosti, obrane, javne sigurnosti te sprječavanje, istrage, otkrivanje i progon kaznenih djela).

Sud se slaže s navodima *Digital Rights* presude da zadržani podatci elektroničke komunikacije mogu omogućiti donošenje vrlo preciznih zaključaka o privatnom životu osoba čiji su podatci zadržani, dok posebno ozbiljnom smatra okolnost da se podatci zadržavaju a da o tome korisnici elektroničkih komunikacija nisu obaviješteni, što može kod njih stvoriti osjećaj da je njihov privatni život predmet trajna nadzora.

7. POSLJEDICE SUDSKE PRAKSE NA UREĐENJE ZADRŽAVANJA PODATAKA U EU-u

Donošenjem presude *Digital Rights* iz 2014. godine, kojom je Direktiva o zadržavanju podataka stavljena izvan snage, ta je Direktiva uklonjena iz pravnog poretka Europske unije. To je imalo za posljedicu da na razini Europske unije više ne postoji propis kojim se uspostavljaju minimalna zajednička pravila u području zadržavanja podataka, odnosno nema jasnih i preciznih pravila o zadržavanju podataka, nema jasnih kriterija pristupa nadležnih tijela podatcima te nema dostatnih jamstava koja omogućuju učinkovitu zaštitu osobnih podataka od rizika zlouporabe. No, to ujedno ne znači da na razini EU-a više ne postoje nikakve odredbe koje se odnose na zadržavanje podataka. Naime, i dalje je na snazi čl. 15., st. 1. Direktive o privatnosti i elektroničkim komunikacijama, ali i niz odredaba iz Povelje o temeljnim pravima. Budući da je direktiva po svojoj pravnoj prirodi propis koji države članice implementiraju u nacionalna zakonodavstva, države članice donijele su nacionalne propise kojima su transponirale Direktivu o zadržavanju podataka u nacionalni pravni poredak. Nakon što je Sud utvrdio da Direktiva o zadržavanju podataka zadire u temeljna prava i slobode, postavilo se pitanje održivosti nacionalnih pravnih propisa o zadržavanju podataka kojima je Direktiva prenesena u nacionalni pravni poredak. Odnosno, postavilo se pitanje u kojoj mjeri i nacionalni propisi zadiru u temeljna prava i slobode te jesu li u suprotnosti s propisima Europske unije koji su na snazi. Nakon presude *Digital Rights* nacionalna zakonodavstva, ostavši bez zajedničkog pravnog okvira,

počela su se razvijati u različitim pravcima tako da je donošenje presude imalo za posljedicu neujednačena pravna uređenja područja zadržavanja podataka.[58]

Upravo zbog izostanka pravne regulative na razini EU-a režimi i politike zadržavanja podataka u Europskoj uniji počeli su se razvijati u tri različita smjera. U nekim državama (Austrija[59], Slovenija i Nizozemska) nacionalni ustavni sudovi ukinuli su nacionalne propise, odnosno odlukom nacionalnog suda nacionalni propisi o zadržavanju podataka više nisu primjenjivi. Neke države (Belgija, Njemačka, Bugarska, Rumunjska, Slovačka, UK) donijele su nove propise[60] odnosno donošenje je novih propisa u tijeku (Irska, Švedska), dok su ostale države (Hrvatska, Cipar, Češka, Danska, Estonija, Finska, Francuska, Grčka, Mađarska, Italija, Latvija, Litva, Luksemburg, Malta, Portugal, Poljska, Španjolska) zadržale postojeće propise u iščekivanju novoga pravnog uređenja na razini Europske unije.[61] Navedeno je za građane EU-a stvorilo situaciju pravne nesigurnosti i postojanja različitih pravnih režima zadržavanja podataka u EU-u kao prostoru slobode, sigurnosti i pravde.

Druga važna posljedica tih dviju presuda Suda EU-a ogleda se u tome da su njima definirani standardi i pretpostavke kojih se nacionalni propisi trebaju pridržavati pri uređivanju područja zadržavanja podataka. Naime, Sud Europske unije ne osporava potrebu i opravdanost prikupljanja i obrade podataka elektroničke komunikacije te dopušta da države članice zadrže, odnosno donesu propise koji ispunjavaju određene uvjete u odnosu na zadržavanje podataka, pristup podatcima, vrijeme zadržavanja i jamstva zaštite.[62] Sud EU-a jasno navodi pretpostavke koje nacionalni propisi moraju ispunjavati da se ne bi smatrali disproporcionalnim zadiranjem u temeljna prava, a te su pretpostavke sljedeće:

1) Zadržavanje podataka mora biti ograničeno, a trajanje razmjerno

Potrebno je omogućiti ciljano zadržavanje podataka o prometu i lokaciji u svrhu borbe protiv teških kaznenih djela uz uvjet da zadržavanje podataka – kad je riječ o kategorijama podataka koji trebaju biti zadržani, određenim komunikacijskim sredstvima, osobama na koje se zadržavanje odnosi kao i njegovu trajanju – bude ograničeno na ono što je strogo nužno.

[58] Više o posljedicama presude *Vedaschi*; *Lubello*, 2015, 30–33; *Stoeva*, 2014, 587–589.

[59] Više o tome *Lehner*, 2014, 445–457.

[60] Više o tome *Munir*; *Yasin*; *Bakar*, 2017, 76–93.

[61] Podatci su dobiveni u okviru rada Radne skupine Vijeća EU-a za razmjenu informacija i zaštitu podataka čiji su ostali detalji povjerljive naravi i ograničeni isključivo na članove Radne skupine (oznaka WK).

[62] Presuda Suda EU-a od 21. prosinca 2016. u spojenim predmetima C-203/15 i C-698/15 (*Tele2*), toč. 108–123.

2) Pristup i upotreba zadržanih podataka moraju biti ograničeni

Potrebno je definirati okolnosti i uvjete u kojima nadležnim nacionalnim tijelima treba biti odobren pristup podatcima. Pristup u načelu može biti odobren s obzirom na cilj borbe protiv kriminaliteta samo podatcima osoba za koje postoji sumnja da namjeravaju počiniti ili su počinile teško kazneno djelo ili da su na kakav drugi način sudjelovale u tom djelu. Bitno je da pristup nadležnih nacionalnih tijela zadržanim podatcima u načelu bude podvrgnut prethodnom nadzoru suda ili neovisnoga upravnog tijela. Također, važno je da nadležna nacionalna tijela kojima je odobren pristup o tome obavijeste osobe o čijim je podatcima riječ čim takva obavijest ne može ugroziti istragu.

3) Potrebna je zaštita od moguće zlouporabe

Potrebno je da pružatelji usluga poduzmu prikladne tehničke i organizacijske mjere koje osiguravaju učinkovitu zaštitu zadržanih podataka od rizika zlouporabe kao i od svakoga nezakonita pristupa tim podatcima.

U odnosu na aktualni zakonodavni okvir RH u vezi sa zadržavanjem podataka posljedice donesenih presuda ogledaju se u potrebi razmatranja svih relevantnih pitanja koje je adresirao Sud u smislu zadržavanja podataka te njihove usklađenosti sa standardima koje je utvrdio u svojim presudama. S obzirom na navedeno sporna je odredba čl. 109. ZEK-a koja propisuje opće i neselektivno zadržavanje podataka u odnosu na sve osobe koje su korisnici komunikacijskih mreža i usluga a da njihovo ponašanje, kako to traži Sud EU-a, nema vezu, čak ni posrednu ili daleku, s teškim kaznenim djelima. U tom je smislu sporna i odredba čl. 19., st. 5. ZSOS-a jer određuje primjenu mjere čuvanja podataka o ostvarenu telekomunikacijskom prometu koji se odnose na sve korisnike usluga. Naime, Sud EU-a ne protivi se da država članica donese propis koji omogućuje ciljano zadržavanje podataka koje – kad je riječ o kategorijama podataka i komunikacijskim sredstvima – bude ograničeno na ono što je strogo nužno. Opće i neselektivno zadržavanje podataka svih korisnika elektroničke komunikacije prelazi granice strogo nužnog i ne može se smatrati opravdanim u demokratskom društvu kao što to zahtijeva članak 15., stavak 1. Direktive 2002/58 u vezi s člancima 7., 8. i 11. Povelje. Prema praksi Suda EU-a trajanje zadržavanja mora biti ograničeno na ono što je strogo nužno. S obzirom na navedeno sporne su odredbe ZEK-a i ZSOS-a koje propisuju razdoblje obveznog zadržavanja podataka od čak godinu dana, što je potrebno preispitati s aspekta strogo nužnog. Sud EU-a postavio je jasne kriterije pristupa podatcima u smislu da se nacionalni propis mora temeljiti na objektivnim kriterijima da bi definirao okolnosti i uvjete u kojima nadležnim tijelima treba biti odobren pristup zadržanim podatcima. Također, bitno je da pristup podatcima bude podvrgnut prethodnom nadzoru suda ili neovisnoga upravnog tijela kao i da nadležna tijela obavijeste predmetne osobe o tome da su njihovi podatci

zadržani čim takva obavijest ne može ugroziti istragu koja se protiv njih vodi. U tom je smislu upitno zadovoljavaju li odredbe ZKP-a koje propisuju pravo okrivljenika na uvid u spis zahtjev Suda da nadležna tijela obavijeste osobu da su joj podatci zadržani.[63] Posebno osjetljiva situacija nastala je za pružatelje usluga koji u skladu s odredbom čl. 118. ZEK-a mogu biti kažnjeni za prekršaj ako ne ispunjavaju svoje obveze zadržavanja podataka elektroničke komunikacije. Međutim, s druge strane, pružatelji usluga, postupajući i dalje po svojoj zakonskoj obvezi zadržavanja podataka, krše pravo EU-a u onom opsegu u kojem je ta obveza suprotna tom pravu. Stoga je potrebno postaviti jasan okvir za pružatelje usluga da bi bili sigurni u svoje zakonito i dopustivo postupanje.

8. STVARANJE PRIKLADNA OKVIRA REŽIMA ZADRŽAVANJA PODATAKA KOJI POŠTUJE TEMELJNA PRAVA GRAĐANA EU-a

Europska komisija iznijela je svoj stav u vezi s uređenjem zadržavanja podataka na nacionalnoj razini nakon što je Sud EU-a ukinuo Direktivu. Kako navodi Europska komisija[64], države članice slobodne su zadržati postojeća nacionalna zakonodavstva ili donijeti nova uz uvjet da su u skladu s primarnim i sekundarnim izvorima prava EU-a.[65] Dakle, Europska komisija podsjetila je da postoje primarni i sekundarni propisi koji uređuju relevantna pitanja što se tiče zadržavanja podataka i pristup njima. Pri tome se pod primarnim propisima misli na Osnivačke ugovore i Povelju o temeljnim pravima kojima se štite ljudska prava, dok se pod sekundarnim izvorima ponajprije misli na Direktivu 2002/58/EZ o privatnosti i elektroničkim komunikacijama.

Imajući u vidu nespornu važnost zadržanih podataka radi borbe protiv terorizma i teških kaznenih djela s jedne strane i potrebu zaštite temeljnih prava i sloboda građana s druge strane, potrebna su daljnja razmatranja načina poboljšanja sustava zadržavanja podataka radi nedvojbena dokazivanja nužnosti mjere zadržavanja te njezine razmjernosti u odnosu na zadiranje u prava građana EU-a, kako to pitanje razmatra Sud Europske unije.

S obzirom na dopuštenost i nužnost režima zadržavanja podataka vrijedno je spomenuti mišljenje nezavisnog odvjetnika Henrika Saugmandsgaardaøea od 19. srpnja 2016. godine u spojenim predmetima koji su doveli do presude *Tele2*. Naime,

[63] Riječ je o člancima 183., 184. i 184.a ZKP-a.

[64] *European Commission statement on national data retention laws*; STATEMENT/15/5654; Brussels, 16 September 2015.

[65] Točnije, odredbama koje reguliraju zaštitu ljudskih prava, direktivama koje se bave pitanjem zaštite osobnih podataka, kao i odredbom čl. 15., st. 1. Direktive 2002/58/EZ o privatnosti i elektroničkim komunikacijama u odnosu na koju se Sud EU-a u presudi *Tele2* osvrnuo i na nacionalna zakonodavstva o zadržavanju podataka.

citirajući Uvodnu izjavu br. 11. Direktive o zadržavanju podataka, prema kojoj Direktiva ne utječe na sposobnost država članica da zakonito presreću elektroničke komunikacije, odnosno da poduzimaju druge mjere ako je to nužno u neku od propisanih svrha te u skladu s Poveljom, nezavisni odvjetnik smatra da namjera zakonodavca Unije nije bila utjecati na pravo država članica da donose mjere za zadržavanje podataka, nego da to pravo uvjetuju određenim zahtjevima koji se osobito odnose na ciljeve i proporcionalnost mjera. Drugim riječima, nezavisni odvjetnik smatra da se za opću obvezu zadržavanja podataka ne mora uvijek, kao takvu, smatrati da prelazi granice onoga što je strogo nužno u borbi protiv teških kaznenih djela, nego da takva obveza prelazi granice onoga što je strogo nužno ako je ne prate jamstva u smislu pristupa podatcima, trajanja zadržavanja te zaštite i sigurnosti podataka. U okviru ocjene nužnosti nezavisni je odvjetnik mišljenja da je potrebno razmotriti bi li u borbi protiv teških kaznenih djela druge mjere bile jednako učinkovite kao opća obveza zadržavanja, pri čemu se u obzir mora uzeti činjenica da takve mjere nadležnim tijelima daju određenu mogućnost da uvidom u podatke promatraju prošlost.[66]

Upravo zbog nepostojanja ujednačena pristupa na razini EU-a, bez propisanih minimalnih standarda radi usklađivanja odredaba država članica koje se odnose na obveze zadržavanja podataka elektroničke komunikacije, pokazuje se potreba da se na razini Europske unije donese propis kojim bi se osiguralo da države članice imaju jedinstven pristup pitanju zadržavanja podataka uz puno poštivanje prava građana EU-a zajamčenih Poveljom. Takav jedinstven i ujednačen zakonodavni okvir ne samo da će pridonijeti harmonizaciji nacionalnih zakonodavstava u području zadržavanja podataka te smanjiti pravne razlike koje postoje između njih, nego će ukloniti moguće rizike koji postoje u činjenici da države članice, bez takvih jedinstvenih pravila i smjernica, izrađuju nacionalne propise kojima se dodatno krše prava građana EU-a zajamčena Poveljom. Nova direktiva trebala bi zaštititi privatnost prava zajamčena građanima EU-a uz postavljanje jasna okvira zadržavanja podataka (i pristupa tim podatcima) radi borbe protiv terorizma i teških kaznenih djela. Taj bi okvir trebao zadovoljiti načela nužnosti, prikladnosti i proporcionalnosti u okviru demokratskog društva. Osim toga, novi instrument EU-a trebao bi uspostaviti definiciju teškoga kaznenog djela i postaviti jasna i nedvojbena pravila u odnosu na svrhu zadržavanja kao i razdoblje u kojem se zadržavaju podatci. Također, novi instrument trebao bi što je više moguće ograničiti broj osoba koje imaju pristup zadržanim podatcima kao i suziti što je više moguće opseg i vrstu podataka koji će se zadržavati. Konačno, mora

[66] Mišljenje nezavisnog odvjetnika Henrika Saugmandsgaardaøea u spojenim predmetima C-203/15 Tele2 Sverige AB/Post-ochtelestyrelsen i C-698/15 Secretary of State for Home Department/Tom Watson i dr. od 19. srpnja 2016. godine, 29.

osigurati kao nužan preduvjet odobrenje suda ili drugoga upravnog tijela kao i dati jasne smjernice za osiguranje i provedbu potrebnih zaštitnih jamstava.[67]

Noviji primjer nacionalnog rješenja pitanja zadržavanja podataka nalazi se u njemačkom zakonodavstvu koje je doneseno u prosincu 2015. godine, a stupilo je na snagu u srpnju 2017. godine (tako dug *vacatio legis* propisan je zbog potrebe prilagodbe pružatelja usluga novu režimu zadržavanja podataka).[68] Novi njemački propisi postavljaju jasnu razliku između obveze zadržavanja podataka i pristupa tim podatcima. Razdoblje zadržavanja podataka smanjeno je na četiri tjedna u odnosu na podatke o lokaciji (s obzirom na njihovu osjetljivost) i deset tjedana u odnosu na podatke o prometu. Što se tiče prometnih podataka, neke vrste tih podataka ne mogu se obvezno zadržavati, poput svih podataka e-pošte i podataka o posjećenim stranicama kao i podataka vezanih uz djelovanje društvenih i crkvenih organizacija koji pružaju telefonsko psihološko savjetovanje. Dakle, Njemačka u biti nije suzila krug osoba čiji se podatci zadržavaju, nego je skratila razdoblje zadržavanja podataka i isključila određene kategorije podataka koji se zadržavaju. Time nije potpuno odgovorila na zahtjeve Suda što se tiče selektivnosti osoba čiji se podatci zadržavaju.

Što se tiče pristupa podatcima, on je moguć samo radi istraga teških kaznenih djela i prevencije ozbiljnih prijetnji javnom interesu. Pristup podatcima razlikuje se ovisno o tome pristupa li se podatcima koje pružatelji usluga zadržavaju u poslovne svrhe (podatci *billing*) ili podatcima koje pružatelji usluga obvezno zadržavaju. Obvezno zadržanim podatcima o prometu mogu pristupiti tužitelji samo u slučaju sumnje da je osoba počinila neko od teških kaznenih djela taksativno navedenih (npr. osnivanje terorističke organizacije, raspačavanje dječje pornografije, ubojstvo, trgovanje ljudima radi seksualnog iskorištavanja). Pristup podatcima moguć je isključivo na temelju sudskog naloga, i to samo onim podatcima koji se tiču osoba koje su osumnjičene ili optužene za počinjenje tih kaznenih djela uz uvjet da su o takvu pristupu obaviještene. Zadržani podatci moraju biti uništeni čim više ne postoji potreba za njima radi kaznenog progona. Novi njemački propis donesen je nakon presude *Digital Rights*, ali prije presude *Tele2* te zbog toga nije potpuno odgovorio na zahtjeve i standarde koje je Sud postavio u smislu zadržavanja podataka. Unatoč tomu navedeni je propis korak naprijed u uređivanju područja zadržavanja podataka te može biti inspiracija u pronalaženju rješenja koja će u većoj mjeri poštivati ljudska prava.

Dana 30. prosinca 2016. godine u Ujedinjenom je Kraljevstvu stupio na snagu novi zakon koji regulira, između ostalog, i pitanje zadržavanja podataka.[69] Prema novom

[67] Više o tome *Stoeva*, 2014, 589–590; *Galli*, 2016, 462–466; *Vaciago*, 2014, 68.

[68] Vidi *Law on the introduction of an obligation to store and a maximum period to retain traffic data (Gesetz für Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten).*

[69] Vidi *Investigatory Powers Act* 2016. Tekst zakona dostupan je na mrežnoj stranici http://www.legislation.gov.uk/ukpga/2016/25/contents/enacted.

zakonu državni tajnik može naložiti pružateljima usluga da zadrže potrebne podatke o elektroničkim komunikacijama samo ako je takvo zadržavanje nužno i razmjerno te radi nacionalne sigurnosti i borbe protiv terorizma i teških kaznenih djela. Nalog o zadržavanju može se odnositi na jednog ili više pružatelja usluga, na sve ili neke vrste podataka. Razdoblje za koje se traži zadržavanje ne može biti dulje od 12 mjeseci od dana komunikacije. Zakon je podvrgnut brojnim i ozbiljnim kritikama jer se i dalje omogućuje neselektivno zadržavanje podataka, pogotovo u odnosu na krug osoba, dok državni tajnik zadržava široku diskreciju u samom nalaganju zadržavanja. Rezultat je kritika da je zakon dobio pogrdni naziv *Snooper's Charter.*

Prema belgijskome nacionalnom rješenju[70] podatci se zadržavaju do šest mjeseci za potrebe istrage i progona terorizma i teških kaznenih djela. Pristup nije moguć bez sudskog naloga. Time nije riješeno pitanje neselektivnosti. Istodobno je u Italiji na iznenađenje europske zajednice u prosincu 2017. godine stupio na snagu zakon prema kojem su pružatelji usluga obvezni zadržavati podatke elektroničke komunikacije 72 mjeseca, odnosno šest godina od dana obavljene komunikacije. Iako je ta obveza propisana kao iznimka od opće obveze pružatelja usluga da zadržavaju podatke 12 – 24 mjeseca, i to u smislu da se toliko duži period propisuje isključivo u svrhu progona određenih kaznenih djela, uključujući kaznena djela međunarodnog terorizma, ostaje otvoreno pitanje kako će pružatelji usluga znati koje bi osobe mogle biti dovedene u vezu s počinjenjem određenih kaznenih djela, pa da bi se u odnosu na njih podatci zadržavali 72 ili 12 – 24 mjeseca. Navedeno se pitanje postavlja to više što talijanski zakon ne pruža mehanizam ciljanog zadržavanja podataka temeljen na postojanju veze pojedine osobe i planiranja ili počinjenja kaznenog djela.[71]

Konačno, korisno je spomenuti i rad radne skupine švedskog Ministarstva pravosuđa, sastavljene od stručnjaka koji provode zakone (*law enforcement*) te sudaca, odvjetnika, predstavnika akademske zajednice i predstavnika vlade kojoj je povjeren zadatak pronalaska prikladna rješenja novoga zakonodavnog okvira u području zadržavanja podataka. Radna skupina smatra da je potrebno revidirati nacionalna pravila u ovom području, međutim uz uvjet da se nikako ne naruši učinkovitost borbe protiv teških kaznenih djela. Mišljenja je da je potrebno ograničiti zadržavanje podataka na ono što je strogo nužno, i to ovako: većina podataka o prometu i lokaciji neće se zadržavati te bi trebalo zadržavati samo one podatke koji su nužni za borbu protiv teških kaznenih djela. Zadržavanje podataka potrebno je razlikovati u odnosu na telefoniju i poruke (zadržavali bi se samo podatci o komunikacijama mobilnim uređajima, dok bi podatci o komunikacijama fiksnom linijom bili isključeni) te u odnosu na internet (zadržavali bi se podatci o IP-adresama i ostali povezani podatci).

[70] Vidi *Law of 29 May 2016 on the collection and retention of data in the telecommunications sector (Loi relative à la collecte et à la conservation des données dans le secteur des communications électroniques).*

[71] *Maggiore*, 2017.

Što se tiče razdoblja zadržavanja podataka, ono bi variralo s obzirom na vrstu podataka; podatci o lokaciji zadržavali bi se najdulje dva mjeseca, podatci o internetu deset mjeseci, a svi ostali podatci šest mjeseci. Pristup zadržanim podatcima bio bi ograničen samo u odnosu na teška kaznena djela te u odnosu na osobe koje su osumnjičene za planiranje ili počinjenje teškoga kaznenog djela. Svaki pristup bio bi odobren na temelju prethodne odluke suda ili neovisnoga upravnog tijela. Budući da švedski nacionalni propis zadovoljava te uvjete, osim u dijelu koji se tiče nacionalne sigurnosti, prijedlog je radne skupine da državni tužitelji budu imenovani kao neovisna upravna tijela koja će odobravati pristup nadležnim službama nacionalne sigurnosti.[72] Nakon što je radna skupina izradila svoje mišljenje, u tijeku je rad na prijedlogu zakona čiji sadržaj u ovom trenutku nije poznat. Ipak, ne možemo se oteti dojmu da je radna skupina obradila problematiku sužavanja opsega podataka kao i skraćivanja razdoblja zadržavanja podataka, dok se nije dotakla pitanja sužavanja kruga osoba u odnosu na koje pružatelji usluga zadržavaju podatke.

Kada se pomno analiziraju presude Suda EU-a, može se zaključiti da će države članice imati najveće poteškoće u implementaciji onih dijelova presude koje se odnose na zadržavanje, dok će se oko reguliranja samog pristupa podatcima i jamstvima od zlouporabe mnogo lakše doći do zadovoljavajućih zakonodavnih rješenja. Naime, u odnosu na pravo pristupa podatcima, države članice moći će ograničiti taj pristup samo za one osobe kojima je to ključno za borbu protiv terorizma i organiziranog kriminala. Slično je i s jamstvima kojima će se osigurati da ne dođe do zlouporabe podataka. No, u odnosu na zadržavanje Sud je postavio zahtjev da ono ne smije biti neselektivno, a upravo ta neselektivnost omogućuje tijelima i otkrivanja i progona da zahvate i one počinitelje koji su tim službama inače izvan neposredna praćenja. Osnovno je pitanje kako propisati uži krug osoba čiji se podatci zadržavaju a da to nema negativna utjecaja na otkrivanje, sprječavanje i procesuiranje terorizma i organiziranog kriminala. Osim toga, iznimno je bitno i pitanje roka zadržavanja podataka, odnosno koje je to minimalno razdoblje koje bi se moglo propisati a da ono ne utječe na učinkovitost istražnih radnji. Također, kada je u pitanju vrsta podataka koja se zadržava, korisno je spomenuti mišljenje austrijskoga Ustavnog suda prema kojem zakonodavac, ako želi zadovoljiti kriterij proporcionalnosti, mora pomno razmotriti sve vrste podataka koje se zadržavaju i njihov stvarni doprinos u prevenciji i rješavanju teških kaznenih djela.[73]

Kako dalje? Ključno je da Europska komisija što prije iziđe u javnost s prijedlogom rješenja nastale situacije. Pri tome mora dati odgovore na pitanja na koja je posebice upozorio Sud EU-a: kako osigurati selektivnost zadržavanja podataka, kako osigurati da pristup podatcima bude ograničen na ono što je nužno te da bude podvrg-

[72] *Ministry of Justice of Sweden* 2017, 34–45.

[73] *Lehner*, 2014, 450.

nut neovisnom nadzoru, kako osigurati dostatna jamstva zaštite podataka od zlouporabe. Također, nužno je donošenje propisa na razini Europske unije kojim bi se osiguralo da države članice imaju jedinstven pristup pitanju zadržavanja podataka uz puno poštivanje prava građana EU-a zajamčenih Poveljom. Konačno, u ovom trenutku postavlja se pitanje državama članicama koji pristup odabrati – čekati ili biti proaktivan? Prednost je čekanja rješenja na razini EU-a da će Republika Hrvatska, pri potrebnim izmjenama nacionalnog zakonodavstva, raspolagati pravnim okvirom zadržavanja podataka kojem će prilagoditi svoje nacionalno zakonodavstvo. S druge strane, nedostatak tog pristupa leži u činjenici da Republika Hrvatska tijekom čekanja europskog rješenja ima i dalje na snazi propise koji su u suprotnosti s kriterijima koje postavlja sudska praksa Suda EU-a. Tako se Republika Hrvatska, a i sve druge države članice koje jednako postupaju, izlažu riziku da nacionalni ustavni sud donese odluke kojom poništava sve propise koji nisu u skladu s izvorima prava EU-a kao i mogućim tužbama fizičkih i pravnih osoba za naknadu nastale štete.

Činjenica da u ovom trenutku od 28 država članica EU-a njih čak 17 i dalje ima na snazi zakonske propise koji omogućuju zadržavanje podataka jasno pokazuje kako je riječ o iznimno važnu, kompleksnu i osjetljivu pitanju u odnosu na koje će biti izazov ispuniti kriterije koje postavlja sudska praksa Suda EU-a. Države članice svjesne su važne uloge i dodane vrijednosti zadržanih podataka u borbi protiv terorizma i organiziranog kriminala.

Europska komisija, koja uz države članice, radi na rješavanju ovog pitanja, još početkom 2017. godine najavila je izradu smjernica za države članice o tome kako konstruirati nacionalna zakonodavstva da bi ona bila u skladu s praksom Suda EU-a, međutim ni danas, godinu dana poslije, ne nazire se rješenje Europske komisije. Zasad je jedino nesporan stav Europske komisije da je očito da tijela za provedbu zakona trebaju imati pristup kritičnoj količini podataka elektroničke komunikacije. Europska komisija smatra da su nacionalna zakonodavstva država članica EU-a u odnosu na pristup podatcima podvrgnuta vrlo jasnim i strogim uvjetima uz nužnost poštivanja temeljnih prava i sloboda, dok najveće izazove vidi u pronalasku rješenja u odnosu na opseg i metodu da pružatelji usluga ciljano zadržavaju podatke.

9. ZAKLJUČAK

Zadržavanje podataka elektroničke komunikacije višeslojno je i kompleksno višedisciplinarno područje. Ne samo da obuhvaća područje javne i nacionalne sigurnosti te kaznenoga procesnog prava nego i područje poštivanja temeljnih ljudskih prava i sloboda. Budući da je nužno osigurati sigurnost svih građana EU-a i njihovu privatnost, potrebno je pronaći pravu ravnotežu između javnog i privatnog interesa. Ljudska prava ne uživaju neograničenu zaštitu, ali svako ograničenje prava i sloboda

može biti opravdano samo ako je potrebno i odgovara ciljevima od općeg interesa. Stoga je nesporno da su borba protiv teških kaznenih djela, organiziranog kriminala i terorizma od iznimne važnosti za zaštitu javne sigurnosti te su time u općem interesu. No, to ne znači da je time i svaka konkretna mjera opravdana i nužna za ostvarivanje tih legitimnih interesa. Da bi zadiranje u ljudska prava zbog javnog interesa bilo opravdano, ono mora biti bitno, a nametnuto ograničenje nužno i razmjerno cilju koji se time nastoji ostvariti. Nije sporno da na razini Europske unije postoji fragmentirano uređenje režima zadržavanja podataka te je potreban jedinstven pristup tom pitanju koji će ukloniti pravnu prazninu nastalu proglašenjem nevaljanom Direktive o zadržavanju podataka. No, zakonodavni instrument trebao bi postaviti minimalne standarde zajedničke za sve države članice Europske unije te jamčiti privatnost građana EU-a uz istodobno jamstvo zaštite od terorizma i teških kaznenih djela.

Od svih pitanja koja je Sud EU-a problematizirao vezano uz pitanje zadržavanja, pristupa i sprječavanja zlouporabe zadržanih podataka, najsloženije je pitanje regulacije zadržavanja podataka, dok se u odnosu na pitanje pristupa podatcima i zaštitnih jamstava od zlouporabe mogu lakše pronaći prihvatljiva rješenja. U odnosu na zadržavanje podataka izdvajaju se dva pitanja. To je selektivnost zadržavanja podataka u odnosu na korisnike telekomunikacijskih sredstava te razdoblje zadržavanja. Posljednje se zapravo odnosi na minimalni rok za zadržavanje a da se pri tome ne našteti učinkovitosti prevencije, otkrivanja i progona teških kaznenih djela. U odnosu na krug osoba čiji bi se podatci trebali zadržavati odgovor se ne nazire. Represivni aparat smatra nužnim da se zadržavaju podatci svih korisnika elektroničke komunikacije, pri čemu sve fizičke osobe, a i većina pravnih osoba, ostaju obuhvaćene obvezom zadržavanja podataka bez obzira na to što se ni posredno neće naći u vezi s počinjenjem teških kaznenih djela. Za selektivno određivanje kruga osoba čiji će se podatci zadržavati ključno bi bilo da nadležne službe država članica posjeduju jake sposobnosti procjene rizika te da na temelju takvih procjena određuju krug osoba čiji će se podatci zadržavati. Pri tome treba biti svjestan da ne mogu postojati takve procjene rizika kojima određeni pojedinci neće promaknuti. Stoga je pitanje jesmo li spremni na taj rizik da bismo sačuvali vlastita temeljna ljudska prava. Nadalje, iz prakse djelovanja represivnog aparata razvidno je da se zadržani podatci ne rabe samo za otkrivanje, progon i procesuiranje terorizma i organiziranog kriminala nego i u slučajevima kao što je, primjerice, nestanak djece. Ako bi se selektivno zadržavali podatci, moramo biti svjesni da oni ne bi bili dostupni za traženje nestalih osoba. Što se pak tiče samog pristupa zadržanim podatcima i jamstava da neće doći do zlouporabe, moguće je pravno unaprijediti propise, ali i samu kontrolu korištenja zadržanim podatcima. Krug ovlaštenih osoba treba biti jasno definiran, pri čemu njihovo pravo pristupa treba biti ovisno o postojanju odobrenja nezavisnog tijela. Zaključno možemo reći da u ovom trenutku nijedna administracija države članice nije našla odgovor na ključno

pitanje kako osigurati selektivnost zadržavanja podataka, dok su rješenja u odnosu na ostala pitanja već riješena ili se mogu riješiti postojećim propisima.

Što se tiče nacionalnih propisa RH kojima se uređuje zadržavanje i pristup podatcima, bit će potrebno izmijeniti one odredbe koje su u suprotnosti s Poveljom i sekundarnim izvorima prava EU-a imajući u vidu zahtjeve sudske prakse Suda EU-a. Treba voditi računa da Republika Hrvatska zadržavanjem na snazi nacionalnih propisa koji ne ispunjavaju kriterije koje je postavio Sud EU-a krši odredbe Povelje o temeljnim pravima EU-a i ostale izvore prava EU-a koji se odnose na zaštitu osobnih podataka. Stoga su moguće sve pravne posljedice koje se redovito vežu uz kršenje europskog prava, uključujući tužbe Europske komisije protiv države članice kao i tužbe pojedinaca na nacionalnim sudovima usmjerene na naknadu štete.[74] U tom kontekstu bilo bi oportuno razmotriti duljinu razdoblja koje prethodi počinjenju ili pokušaju kaznenog djela, a u kojem se najintenzivnije akumuliraju podatci koje bi bilo korisno zadržavati. Prema aktualnim okvirnim procjenama, što nacionalnih, što europskih tijela za provedbu zakona (*law enforcement*), zadržani podatci koji se u najvećoj mjeri upotrebljavaju za potrebe istraga i kaznenog progona datiraju šest mjeseci od počinjenja ili pokušaja kaznenog djela. Navedeno znači da bi *de lege ferenda*, posebice u Republici Hrvatskoj, valjalo razmotriti izmjene pozitivnih zakonskih propisa koji reguliraju pitanje razdoblja u kojem su pružatelji usluga, odnosno operatori obvezni zadržati podatke elektroničke komunikacije. Smanjenjem razdoblja od 12 mjeseci (što trenutačno vrijedi) na šest mjeseci naše nacionalno zakonodavstvo približilo bi se zahtjevima koje postavlja sudska praksa Suda EU-a, s time da se ne bi narušila dosadašnja učinkovitost prevencije, otkrivanja i progona teških kaznenih djela. Također, u odnosu na pristup nacionalnih tijela zadržanim podatcima, koji prema kriterijima koje postavlja Sud EU-a treba biti podvrgnut prethodnom nadzoru neovisnog tijela, pokazuje se potreba da se dodatno analiziraju odredbe Zakona o policijskim poslovima i ovlastima s obzirom na to da ne postavljaju prethodni nadzor neovisnog tijela kao preduvjet policijskog pristupa zadržanim podatcima.

Presuda *Tele2* donesena je prije manje od dvije godine. Otada su vođene brojne rasprave na razini EU-a i na nacionalnoj razini država članica. Za sada rasprave nisu urodile konkretnim zakonskim prijedlozima koji bi na odgovarajući način uvažili stavove Suda oko zadržavanja podataka. Dio država članica odlučio se za čekanje prijedloga Europske komisije za buduće uređenje područja zadržavanja podataka da bi potom pristupile promjenama nacionalnih propisa. No, za to vrijeme i dalje su na snazi nacionalni propisi koji zabrinjavajuće zadiru u privatnost osoba te u ljudska prava pojedinaca. Upravo zbog toga sve države članice trebale bi pojačati napore da bi se što prije došlo do pravnog uređenja zadržavanja podataka koje neće prelaziti ono što je nužno za učinkovito sprečavanje organiziranog kriminala i terorizma.

[74] Vidi *Goldner Lang*; *Perišin*; *Vasiljević*; *Mataija*; *Carević*; *Kuhta*, 2014, 8–9.

LITERATURA

1. Blakeney, S. (2007). The Data Retention Directive: combating terrorism or invading privacy?. Computer and Telecommunications Law Review, 1–7.
2. Dragičević, D.; Gumzej, N. (2014). Obvezno zadržavanje podataka i privatnost. Zbornik Pravnog fakulteta u Zagrebu, Vol. 64, No.1, 39–79.
3. Drewry, L. (2016). Crimes without culprits: Why the European union needs data retention, and how it can be balanced with the right to privacy. Wisconsin International Law Journal, 728–753.
4. Galli, F. (2016). Digital Right Ireland as an opportunity to foster a desirable approximation of data retention provisions. Maastricht Journal of European and Comparative Law, 460–477.
5. Goldner Lang, I.; Perišin, T.; Vasiljević, S.; Mataija, M.; Carević, M.; Kuhta, F. (2014). Pravno mišljenje članova Katedre za europsko javno pravo Pravnog fakulteta Sveučilišta u Zagrebu o pravnim posljedicama presude Suda EU-a u spojenim predmetima C-293/12 i C-594/12 na Republiku Hrvatsku, 1–13.
6. Lehner, A. (2014). Data Retention: A Violation of the Right to Data Protection – An analysis of how the Constitutional Court applied the fundamental right to data protection. ICL Journal, 445–457.
7. Lynskey, L. (2014). The Data Retention Directive is incompatible with the rights to privacy and data protection and is invalid in its entirety. Common Market Law Review 51, 1789–1812.
8. Maggiore, M. (2017). The New Data Retention Provisions In Italy: From Bad To Worse. Dostupno na: http://www.mmlex.it/the-new-data-retention-provisions-in-italy-from-bad-to-worse/.
9. Ministry of Justice of Sweden (2017). Datalagring – brottsbekämpningochintegritet. Dostupno na: http://www.regeringen.se/4a8d12/contentassets/b635202b96fc4e4490886e0ef8601e66/datalagring--brottsbekampning-och-integritet-sou-201775, 34–45.
10. Munir, A. B.; Yasin, S. H. M.; Bakar, S. S. A. (2017). Data Retention Rules: A Dead End?. European Data Protection Law Review, 71–83.
11. Stoeva, E. (2014). The data Retention Directive and the right to privacy. ERA forum, 575–592.
12. Tracol, X. (2014). Legislative genesis and judicial death of a directive: The European Court of Justice invalidated the data retention directive (2006/24/EC) thereby creating a sustained period of legal uncertainty about the validity of national laws which enacted it. Computer Law and Security Review, 736–746.
13. Turkalj, K., (2011). Pravni i institucionalni okvir Europske unije za suzbijanje terorizma, disertacija, Zagreb, 82–101.
14. Turkalj, K. (2002). Borba protiv terorizma na razini Europske unije. Hrvatska pravna revija 2: 10, 1–15.

15. Vaciago, G. (2014). The Invalidation of the Data Retention Directive – A first impact assessment of the CJEU decisions in the joint cases, C293/12 and C-594/12. Computer Law Review, 65–69.
16. Vedaschi, A.; Lubello, V. (2015). Data Retention and its implications for the fundamental right to privacy. Tilburg Law Review, 14–34.

Summary

CHALLENGES TO LEGAL SOLUTIONS OF DATA RETENTION OF ELECTRONIC COMMUNICATION IN THE LIGHT OF RECENT JURISPRUDENCE OF THE COURT OF JUSTICE OF THE EU

The data retention regulatory framework has been one of the most pressing issues in the European Union for the past few years. The main challenge for the EU and its Member States has been to strike a balance between security requirements by taking measures against terrorism and organized crime, and ensuring the protection of human rights and fundamental freedoms. Following the terrorist attacks in the United States and Europe at the beginning of the last decade, the need for introducing the obligation to collect and retain electronic communications data has been identified for the purpose of more effective suppression of terrorism and serious criminal offences. Legislative initiatives at the EU level have resulted in the adoption of regulations setting out a framework for data retention. It is indisputable that data retention is a very useful and effective means for preventing, detecting, investigating and prosecuting criminal offenses. However, at the same time it represents an extremely "invasive" interference with the fundamental rights and freedoms. In particular, it concerns the right to privacy and the right to freedom of expression, guaranteed by the Charter of Fundamental Rights. The European Court of Justice in its judgments Digital Rights and Tele2 pointed out a violation of fundamental rights in the EU and Member States data retention legislation. The paper analyses the scope and impact of the judgments in question on the national legislation and analyses the key human rights standards regarding data retention that the European Court of Justice has identified in its decisions. After the ECJ judgment, the EU member states, including the Republic of Croatia, have faced a major challenge in improving the legal framework for data retention. In this respect, an analysis of the relevant domestic legal framework is provided, as well as the need to review certain solutions for the purpose of full compliance with the requirements and criteria set by the ECJ.

***Key words**: EU, acquis, data retention, European Court of Justice, Data Retention Directive, traffic data, secrecy of communications, security, terrorism, privacy, personal data protection*