UDK: 351.817
Primljeno: veljača 2016.

DAMIR JURAS*, ANTONIO VULAS**

Pravni okvir provjere uspostavljanja telekomunikacijskog kontakta***

Sažetak

U radu se daje prikaz pravnih propisa koji reguliraju obradu i korištenje podataka nastalih elektroničkom komunikacijom, posebice telekomunikacijskih podataka potrebnih za rad na sprječavanju i otkrivanju najtežih oblika kaznenih djela. Posebnu pozornost daje se prikazu presude Europskog suda u Luksemburgu kojom je proglašena nevaljanom Direktiva koja uređuje područje proizvodnje i obrade telekomunikacijskih podataka, te se ističe da je Republika Hrvatska novelama zakonodavstva pravno područje provjere uspostavljanja telekomunikacijskih kontakata regulirala u skladu sa smjernicama Europskog suda koji je upozorio na neusklađenost navedene Direktive s pravima na poštovanje privatnosti i zaštitu osobnih podataka.

Ključne riječi: *Direktiva 2006/24/EZ, Europski sud, nadzor telekomunikacija, policija, provjera telekomunikacijskog kontakta.*

---

* dr. sc. Damir Juras, dipl. iur., voditelj Odjela disciplinskog sudovanja Ministarstva unutarnjih poslova u Splitu.

** Antonio Vulas, dipl. iur., voditelj Odjela za nezakonite migracije Policijske uprave splitsko-dalmatinske. Autori u tekstu iznose osobna stajališta.

*** Rad se bavi značajnom temom uspostavljanja telekomunikacijskih kontakata i tema će zasigurno biti od interesa čitateljstvu i stručnoj javnosti. U obradi navedene teme autori uglavnom koriste deskriptivnu i faktografsku razinu, navodeći dijelove poznatih zakonskih odredbi i razvoja hrvatskog zakonodavstva ili presude Europskog suda iz 2014. Kod opisa hrvatskog uređenja se opisuje razvoj bez dubljeg ulaska u razloge premještanja ove radnje od izvidnih radnji, među policijsko zakonodavstvo te potom među dokazne radnje u ZKP. Takvo premještanje je pobuđivalo brojne teorijske i praktične dvojbe, od dokaznog statusa do pitanja razlike sadašnjeg dvojnog normiranja istovrsnih radnji u policijskom i kazneno-procesnom zakonodavstvu. Direktivu o zadržavanju također obrađuju na razini prikaza, a jednako tako i odluku Europskog suda o kojoj ne donosi podrobnija stajališta. Najznačajniji dio rada su sekundarni podaci o broju zahtjeva po ZPPO i ZKP pri čemu su autori imali prigodu opširnije ih analizirati i oko njih izraditi tekst dok se postojećim pristupom navedeni podaci izgubili u tekstu o drugim područjima bez zasluženog komentara ili osvrta, npr. međusobna usporedba ili usporedba s učestalošću provedenih drugih radnji te izvođenja zaključka o ulozi ovih radnji u istraživanju.

I. UVOD

Počinitelji kaznenih djela se u izvršavanju tih djela koriste razvojem tehničkih mogućnosti i oblika komunikacije, pa je nužno stvoriti pravni okvir koji će, uz poštovanje ljudskih prava na privatnost i zaštitu osobnosti, omogućiti tijelima kaznenog progona da prikupljaju i koriste podatke o kontaktima koje počinitelji kaznenih djela ostvaruju telekomunikacijskim kontaktima[1].

Provjera uspostavljanja telekomunikacijskih kontakata uspostavljenih u određenom razdoblju odnosi se samo na određene telekomunikacijske adrese, određeno vremensko razdoblje i samo na činjenicu uspostavljanja veze. U njenim se okvirima ne mogu prikupljati podaci o sadržaju telekomunikacijskih poruka (Pavišić, 2005: 245; Tomašević et al., 2005).

Novelom Zakona o kaznenom postupku (dalje: ZKP) krajem 2013. (Zakon o izmjenama i dopunama ZKP-a, NN 145/13.) provjera uspostavljanja telekomunikacijskog kontakta je uvedena u poglavlje XVIII. (Dokazne radnje[2]) ZKP-a, NN 152/08., 76/09., 80/11., 121/11., 91/12., 143/12., 56/13., 145/13., gdje je zadržana i posljednjom novelom ZKP-a, NN 152/14.

Odlukom Europskog suda od 8. 4. 2014., u spojenim predmetima C-293/12 i C-594/12 (http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d0f130d6ec5777fd78fb43099fc2c2f4cc0925b1.e34KaxiLc3eQc40LaxqMbN4OaNiRe0?text=&docid=150642&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=87158), Direktiva 2006/24/EZ (SL L 105, 13. 4. 2006.) Europskog parlamenta i Vijeća od 15. ožujka 2006. o zadržavanju podataka proizvedenih ili obrađenih u vezi s pružanjem javno dostupnih elektroničkih komunikacijskih usluga ili javnih komunikacijskih mreža te o dopuni Direktive 2002/58/EZ (SL L 201, 31. 7. 2002.) proglašena je nevaljanom.

II. ZAKONODAVSTVO REPUBLIKE HRVATSKE

Do 2002. godine policija je svoje zahtjeve prema davateljima telekomunikacijskih usluga temeljila na odredbi članka 177. stavka 2. ZKP-a, NN 110/97., 27/98., 58/99., 112/99., koja je predviđala 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[3], izrijekom je kao ovlast policije u provedbi izvida

---

[1] "(…) nakon analitičke obrade izlista telefonskih poziva dobivamo cjelovitu sliku o intenzitetu i trajanju ostvarenih kontakata, posrednim ili neposrednim vezama krajnjih korisnika telefonskih uređaja/linija, mogućim lokacijama baznih stanica na kojima je "logiran" mobilni telefonski uređaj u momentu kontakta (taj podatak se u praksi koristi kao moguća približna lokacija korisnika mobilnog telefonskog uređaja u trenutku kada je ostvarena neka telekomunikacijska usluga), broju odaslanih i primljenih poruka (SMS, MMS) i dr.", Kralj, 2009: 174.-175.

[2] Provjera uspostavljanja telekomunikacijskog kontakta je dokazna radnja iz čega slijedi da ona može biti dokaz u kaznenom postupku., Pavišić, 2015: 429.

[3] Zakonom o izmjenama i dopunama ZKP-a, NN 58/02., čl. 76. noveliran je čl. 177. Zakona, pa je čl. 177. st. 2. od tada glasio: "Radi ispunjenja zadataka iz stavka 1. ovoga članka redarstvene vlasti mogu tražiti potrebne obavijesti od građana, primijeniti poligrafsko testiranje, analiziranje glasa, obaviti potreban pregled prijevoznih sredstava, osoba i prtljage, za prijeko potrebno vrijeme nadzirati i ograničiti kretanje određenih osoba na određenom prostoru (promatranje, pratnja, blokada, racija, zasjeda, klopka, nadzor prijenosa stvari i

kaznenih djela propisano i utvrđivanje istovjetnosti telekomunikacijskih adresa koje su u određenom razdoblju uspostavile vezu[4].

ZKP, NN 152/08., koji je stupio na snagu 2009. godine, u članku 207. propisao je da policija, kad poduzima izvide kaznenih djela postupa prema odredbama posebnog zakona i pravila koja su donesena na temelju tog Zakona.

Zakon o policijskim poslovima i ovlastima (dalje: ZPPO), NN 76/09., 92/14., u članku 68. stavcima 1.-3. propisao je da policija, na temelju pisanog odobrenja načelnika Uprave kriminalističke policije ili načelnika Policijskog nacionalnog ureda za suzbijanje korupcije i organiziranog kriminaliteta ili načelnika policijske uprave, a u njihovoj odsutnosti osoba koje ih zamjenjuju, može od davatelja komunikacijskih usluga zatražiti 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[5]. Navedena provjera može obuhvaćati i utvrđivanje položaja komunikacijskog uređaja, utvrđivanje mjesta na kojima se nalaze osobe koje uspostavljaju elektroničku komunikaciju[6] te identifikacijske oznake uređaja[7].

Člankom 103. Pravilnika o načinu policijskog postupanja, NN 89/10., 78/14., 76/15., propisano je da se provjera uspostavljanja elektroničke komunikacije provodi kroz aplikaciju računalnog sustava za upravljanje zahtjevima za provjeru uspostavljanja elektroničke komunikacije. Ovlaštenici za podnošenje zahtjeva za provjeru uspostavljanja elektroničke komunikacije su: policijski službenik za obradu kriminaliteta; načelnik Operativno-komunikacij-

dr.), poduzeti potrebne mjere u svezi s utvrđivanjem istovjetnosti osoba i predmeta, raspisati potragu za osobom i stvarima, u nazočnosti odgovorne osobe obaviti pregled određenih objekata i prostorija državnih tijela, pravnih osoba te drugih poslovnih prostora i ostvariti uvid u određenu njihovu dokumentaciju i podatke, prikupljati obavijesti uz prikrivanje svrhe prikupljanja ili s prikrivanjem svojstva policijskog službenika, putem tajnog izvjestitelja, od pravne osobe koja pruža telekomunikacijske usluge zatražiti provjeru istovjetnosti telekomunikacijskih adresa koje su u određenom razdoblju uspostavile vezu, te poduzeti druge potrebne mjere i radnje. O činjenicama i okolnostima koje su utvrđene prilikom poduzimanja pojedinih radnji, a mogu biti od interesa za kazneni postupak, sastavit će se službena zabilješka."

[4] U svojem je komentaru Krapac (2002: 189) naveo kako se izmjenama i dopunama ZKP-a 2002. godine povećao katalog izvidnih radnji redarstvenih vlasti, ustanovivši na taj način pravnu osnovu za neke radnje kojima se ograničavaju prava i slobode građana (uporaba tajnog izvjestitelja, provjera istovjetnosti telekomunikacijskih adresa). Podatke o broju zahtjeva za pribavljanje podataka o istovjetnosti telekomunikacijskih adresa, usporedno s brojem kaznenih djela, te brojem telefonskih linija nepokretne mreže i brojem korisnika pokretne telefonske mreže, za razdoblje 2001.-2007., vidi u: Kralj, 2009: 175.

[5] "(…) važno je istaknuti vrijednost prethodnih radnji utvrđivanja istovjetnosti telekomunikacijskih adresa. Na taj način se prethodno potvrđuje ili eliminira određena telekomunikacijska adresa (telefonski broj) u odnosu na intenzitet kontakata s nekom drugom telekomunikacijskom adresom. Takve radnje su u duhu odredaba Zakona o kaznenom postupku, jer potvrđuju načelo supsidijarnosti i neophodnosti u pogledu poduzimanja mjera posebnih dokaznih radnji.", Veić et al., 2009: 94.

[6] Ravnatelj Državne uprave za zaštitu i spašavanje donio je Standardni operativni postupak za djelovanje jedinstvenog operativno-komunikacijskog centra (Centra 112) kod dostave podataka o lokaciji korisnika za pozive iz mreža pokretnih telekomunikacija, http://www.duzs.hr/page.aspx?PageID=608

[7] Odobrenje se temelji na činjenicama iz kojih je vidljivo da se drugim radnjama nije mogao ili se neće moći postići cilj policijskog posla ili bi postizanje tog cilja bilo povezano s nerazmjernim teškoćama. Iznimno, ako je to potrebno radi sprječavanja neposredne opasnosti ili nasilja odnosno radi žurnog traganja za osobama, odobrenje može biti dano i usmeno, ali mora biti pisano potvrđeno najkasnije u roku od 24 sata od danog usmenog odobrenja. (Čl. 68. st. 4. i 5. ZPPO-a.)

skog centra policije; voditelj smjene Operativno-komunikacijskog centra policije; pomoćnik voditelja smjene Operativno-komunikacijskog centra policije. Zahtjev odobrava ovlašteni potpisnik na temelju prethodne suglasnosti ovlaštenih rukovoditelja, i to: načelnika Sektora u Upravi kriminalističke policije; voditelja Službe u Upravi kriminalističke policije; načelnika Sektora/voditelja Službe kriminalističke policije u policijskoj upravi; voditelja Službe/Odjela/Odsjeka u kriminalističkoj policiji policijske uprave; načelnika policijske postaje[8].

Prema evidencijama Ministarstva unutarnjih poslova Republike Hrvatske[9], tijekom 2014. i 2015. godine podnijeto je ukupno 48 460 zahtjeva za provjeru uspostavljanja telekomunikacijskih kontakata na temelju članka 68. ZPPO-a (25 263 zahtjeva 2014. g. i 23 197 zahtjeva 2015. g.), koje su odobrili ovlaštenici u skladu sa zakonskim propisima, nakon čega je izvršena provjera traženih podataka kod davatelja usluga – telekomunikacijskih operatera.

Temeljem članka 33. Zakona o sigurnosno-obavještajnom sustavu (dalje: ZSOS), NN 79/06., 105/06., Sigurnosno-obavještajna agencija prema građanima i Vojna sigurnosno-obavještajna agencija prema zaposlenicima odnosno pripadnicima Ministarstva obrane i Oružanih snaga, mogu primjenjivati mjere tajnog prikupljanja podataka kojima se ograničavaju neka ustavna ljudska prava i temeljne slobode, i to ako se podaci ne mogu prikupiti na drugi način ili je njihovo prikupljanje povezano s nerazmjernim teškoćama. Kao jedna od mjera tajnog prikupljanja podataka propisan je tajni nadzor telekomunikacijskih usluga, djelatnosti i prometa i to kroz: a) tajni nadzor sadržaja komunikacija, b) tajni nadzor podataka o telekomunikacijskom prometu, c) tajni nadzor lokacije korisnika, d) tajni nadzor međunarodnih telekomunikacijskih veza. Člancima 36. i 38. ZSOS-a propisano je da tajni nadzor sadržaja komunikacija pisanim obrazloženim nalogom odobrava sudac Vrhovnog suda Republike Hrvatske, dok ostale oblike tajnog nadzora telekomunikacijskih usluga, djelatnosti i prometa odobravaju ravnatelji sigurnosno-obavještajnih agencija pisanim i obrazloženim nalogom u

[8] Temeljem čl. 102.a st. 1. ZPPO-a, građanski nadzor nad primjenom policijske ovlasti provjere uspostavljanja elektroničke komunikacije ovlašteno je provoditi Vijeće za građanski nadzor nad primjenom pojedinih policijskih ovlasti. Nadzor se može provoditi nakon dovršetka kriminalističkog istraživanja tijekom kojeg je primijenjena policijska ovlast provjere uspostavljanja elektroničke komunikacije. Prilikom obavljanja nadzora Vijeće je ovlašteno od Operativno-tehničkog centra za nadzor telekomunikacija zatražiti usporedbu podataka s kojima raspolaže s podacima Ravnateljstva policije o primijenjenoj ovlasti. U obavljanju nadzora Vijeće može vršiti uvid u izvješća i druge dokumente policije, tražiti pisana očitovanja, a radi objašnjenja navoda iz očitovanja može obaviti razgovore s rukovoditeljima i policijskim službenicima koji su primjene ovlasti odobrili i primjenjivali. Izvješće o saznanjima i podacima prikupljenim u obavljanju nadzora Vijeće će dostaviti u roku od 15 dana predsjedniku Hrvatskog sabora, predsjednicima Odbora za unutarnju politiku i nacionalnu sigurnost i Odbora za ljudska prava i prava nacionalnih manjina Hrvatskog sabora, ministru unutarnjih poslova i glavnom ravnatelju. O izvršenom nadzoru izvješćuje se podnositelj zahtjeva. Nadzor Vijeće provodi na temelju: programa nadzora koji utvrđuje Hrvatski sabor na prijedlog Odbora za unutarnju politiku i nacionalnu sigurnost i uz prethodno pribavljeno mišljenje Odbora za ljudska prava i prava nacionalnih manjina; zahtjeva građana koji smatraju da su im nezakonitom primjenom policijske ovlasti provjere uspostavljanja elektroničke komunikacije povrijeđena prava; zahtjeva državnih tijela i pravnih osoba u vezi sa sumnjom na nezakonitu primjenu ovlasti. Vijeće je sastavljeno od pet članova i pet zamjenika članova, predstavnika građana, koje imenuje i razrješuje Hrvatski sabor na temelju javnog poziva na prijedlog organizacija civilnog društva te znanstvenih i stručnih organizacija (čl. 102. a-c ZPPO-a).; Odbor za unutarnju politiku i nacionalnu sigurnost Hrvatskog sabora je u službenom glasilu Republike Hrvatske, NN 19/16., dana 2. ožujka 2016. objavio Javni poziv za podnošenje prijedloga za imenovanje pet članova i pet zamjenika članova Vijeća za građanski nadzor nad primjenom pojedinih policijskih ovlasti.

[9] Izvor podataka: dopis Ravnateljstva policije, broj: 511-01-43-152-23/16 od 8. ožujka 2016.

okviru propisanog djelokruga[10].

Dopunom ZKP-a članak 339.a, NN 145/13., kojim se provjera uspostavljanja elektroničkog komunikacijskog kontakta regulira ZKP-om kao dokazna radnja, napravljen je bitan korak u zaštiti privatnosti vlasnika ili korisnika komunikacijskih uređaja[11], a dodatna zaštita odnosno sigurnost osigurana je novelom člankom 339.a ZKP-a, NN 152/14. Ako postoji sumnja da je registrirani vlasnik ili korisnik telekomunikacijskog sredstva počinio kazneno djelo u odnosu na koje se mogu provoditi posebne dokazne radnje[12] ili neko drugo kazneno djelo za koje je propisana kazna zatvora teža od pet godina policija može, na temelju naloga suca istrage, a radi prikupljanja dokaza, putem OTC-a[13] od operatora javnih komunikacijskih usluga zatražiti provjeru istovjetnosti, trajanja i učestalosti komunikacije s određenim

[10] U svrhu ostvarivanja građanskog nadzora nad radom sigurnosno-obavještajnih agencija osniva se Vijeće za građanski nadzor sigurnosno-obavještajnih agencija (dalje: Vijeće). Vijeće se sastoji od predsjednika i šest članova koje imenuje Hrvatski sabor. Za članove Vijeća mogu biti imenovani hrvatski državljani visoke stručne spreme, pri čemu najmanje po jedan član Vijeća mora biti diplomirani pravnik, diplomirani politolog i dipl. ing. elektrotehnike. Vijeće obavlja sljedeće poslove: prati zakonitost rada sigurnosnih službi, prati i nadzire primjenu mjera tajnog prikupljanja podataka kojima se ograničavaju ustavna ljudska prava i temeljne slobode, prikupljena saznanja i podatke iz prethodnih točki dostavlja u formi obavijesti Vijeću za nacionalnu sigurnost, predsjedniku Hrvatskoga sabora, predsjedniku odbora Hrvatskoga sabora nadležnog za nacionalnu sigurnost, ravnateljima sigurnosno-obavještajnih agencija, te daje obavijest i o načinu podnošenja zahtjeva građana za obavljanje nadzora. U obavljanju navedenih poslova Vijeće može vršiti uvid u izvješća i druge dokumente sigurnosno-obavještajnih agencija, obavljati razgovore s čelnicima i službenim osobama sigurnosno-obavještajnih agencija, kada je to nužno radi utvrđenja činjenica odlučnih za ocjenu zakonitosti rada agencija. Vijeće navedene poslove obavlja na temelju programa koji donosi odbor za nacionalnu sigurnost; na temelju zahtjeva građana, državnih tijela i pravnih osoba o zamijećenim nezakonitim postupcima ili nepravilnostima u radu sigurnosno-obavještajnih agencija, osobito u slučajevima kršenja Ustavom zajamčenih ljudskih prava i temeljnih sloboda. O izvršenom nadzoru izvješćuje se podnositelj zahtjeva (čl. 110.-113. ZSOS-a).; Odbor za unutarnju politiku i nacionalnu sigurnost Hrvatskog sabora je u službenom glasilu Republike Hrvatske, NN 17/16., dana 24. 2. 2016. objavio Javni poziv za prikupljanje prijedloga za imenovanje predsjednika i šest članova Vijeća za građanski nadzor sigurnosno-obavještajnih agencija.

[11] "S obzirom na stupanj zahvata u temeljna ljudska prava, koji je znatno viši nego što je to slučaj kod ostalih izvidnih radnji, provjera uspostavljanja telekomunikacijskog kontakta koji se vrši radi prikupljanja dokaza i otkrivanja počinitelja kaznenih djela za koji se kazneni postupak pokreće po službenoj dužnosti se sada dijelom uređuje u Zakonu o kaznenom postupku te se jamči viši stupanj zaštite temeljnih prava registriranih vlasnika ili korisnika uređaja, osobito prava na privatnost.", Obrazloženje Prijedloga zakona o izmjenama i dopunama Zakona o kaznenom postupku, PZE 488, http://www.sabor.hr/prijedlog-zakona-o-izmjenama-i-dopunama-zakona-o-k

[12] Člankom 334. ZKP-a određen je katalog kaznenih djela u odnosu na koja se mogu provoditi posebne dokazne radnje određene člankom 332. ZKP-a, a kojim radnjama se privremeno ograničavaju određena ustavna prava građana.

[13] Radi obavljanja aktivacije i upravljanja mjerom tajnog nadzora telekomunikacijskih usluga, djelatnosti i prometa te ostvarivanja operativno-tehničke koordinacije između pravnih i fizičkih osoba koje raspolažu javnom telekomunikacijskom mrežom i pružaju javne telekomunikacijske usluge i usluge pristupa u Republici Hrvatskoj i tijela koja su ovlaštena za primjenu mjera tajnog nadzora telekomunikacija u skladu sa Zakonom o sigurnosno-obavještajnom sustavu (dalje: ZSOS) i ZKP-om, osniva se OTC, koji u suradnji s tijelima koja su ovlaštena za primjenu mjera tajnog nadzora telekomunikacija u skladu sa ZSOS-om i ZKP-om ima ovlast nadzora rada davatelja telekomunikacijskih usluga u smislu izvršenja obveza iz ZSOS-a. OTC za potrebe sigurnosno-obavještajnih agencija i redarstvenih tijela aktivaciju i upravljanje mjerom tajnog nadzora telekomunikacijskih usluga, djelatnosti i prometa obavlja putem odgovarajućega tehničkog sučelja (čl. 18. ZSOS-a, NN 79/06., 105/06.).

elektroničkim komunikacijskim adresama[14], utvrđivanje položaja komunikacijskog uređaja, utvrđivanje mjesta na kojima se nalaze osobe koje uspostavljaju elektroničku komunikaciju, te identifikacijske oznake uređaja. Na temelju naloga suca istrage, putem Operativno-tehničkog centra za nadzor telekomunikacija, istu provjeru policija može zatražiti od operatora javnih komunikacijskih usluga za registriranog vlasnika ili korisnika telekomunikacijskog sredstva koji je povezan s osobom za koju postoji sumnja da je počinila kazneno djelo u odnosu na koje se mogu provoditi posebne dokazne radnje ili neko drugo kazneno djelo za koje je propisana kazna zatvora teža od pet godina. Nalog za navedenu provjeru sudac istrage izdaje na temelju obrazloženog prijedloga nadležnoga državnog odvjetnika. Odluku o zahtjevu državnog odvjetnika sudac istrage dužan je donijeti u roku od četiri sata. Iznimno, ako postoji opasnost od odgode i ako državni odvjetnik ima razloga vjerovati da na vrijeme neće moći pribaviti nalog suca, nalog za provjeru može izdati nadležni državni odvjetnik, koji takav nalog i dopis, u kojem će obrazložiti razloge za njegovo izdavanje, mora odmah, a najkasnije u roku od 24 sata od izdavanja, dostaviti sucu istrage. Sudac istrage odlučuje rješenjem o zakonitosti naloga državnog odvjetnika u roku od 48 sati od primitka naloga i dopisa, a protiv rješenja suca istrage državni odvjetnik nema prava žalbe. U nalogu za provjeru uspostavljanja telekomunikacijskog kontakta, uz podatke iz članka 168. stavka 2. ZKP-a[15], navode se osobni podaci osobe koja je registrirani vlasnik ili korisnik komunikacijskog sredstva te svrha radi koje se nalog izdaje. Nalog za provjeru uspostavljanja telekomunikacijskih kontakata nije potreban, ako je registrirani vlasnik ili korisnik komunikacijskog sredstva dao pisani pristanak. Ako su podaci o uspostavljanju telekomunikacijskog kontakta pribavljeni bez naloga suca istrage odnosno ako državni odvjetnik nije u propisanom roku dostavio sucu istrage nalog ili ako je odbijen zahtjev državnog odvjetnika za ovjeru naloga za provjeru uspostavljanja telekomunikacijskih kontakata, tako prikupljeni podaci ne mogu se upotrijebiti kao dokaz u postupku.

Ministarstvo unutarnjih poslova Republike Hrvatske tijekom 2014. i 2015. godine podnijelo je ukupno 892 zahtjeva za provjeru uspostavljanja telekomunikacijskih kontakata u skladu s člankom 339.a ZKP-a (435 zahtjeva 2014. g. i 457 zahtjeva 2015. g.)[16], koji su odobreni od strane ovlaštenika u skladu sa zakonskim propisima, nakon čega je izvršena provjera traženih podataka kod davatelja usluga – telekomunikacijskih operatera.

Zakon o elektroničkim komunikacijama, NN 73/08., 90/11., 133/12., 80/13., 71/14., koji je usklađen i s Direktivama 2002/58/EZ i 2006/24/EZ (čl. 1.a Zakona), među inim, regulira područje elektroničkih komunikacija, i to korištenje elektroničkih komunikacijskih mreža i pružanje elektroničkih komunikacijskih usluga, pružanje univerzalnih usluga te zaštitu prava korisnika usluga, zaštitu podataka, sigurnosti i cjelovitosti elektroničkih komunikacij-

[14] "Kada govorimo o utvrđivanju istovjetnosti telekomunikacijskih adresa ne smijemo se ograničiti isključivo na komunikaciju telefonom. Suvremeni oblici elektronske komunikacije iz dana u dan se sve više razvijaju, pa u istu kategoriju komunikacija već odavno možemo svrstati komunikaciju internetom (e-mail, Voice Over Internet Protocol, skr. VOIP usluge i dr.). Davatelji internetskih usluga evidentiraju tzv. IP (Internet Protocol) adrese, a njihovim utvrđivanjem moguće je utvrditi istovjetnost krajnjeg korisnika internetskih usluga.", Kralj, 2009:172.

[15] Uvod rješenja ili naloga uvijek sadrži: 1. naziv tijela, 2. ime, prezime i svojstvo službene osobe koja je donijela, odnosno osoba koje su donijele rješenje ili nalog, 3. ime i prezime zapisničara, ako je odluka donesena u zasjedanju, 4. ime i prezime okrivljenika te identifikacijski broj građana, 5. kazneno djelo koje je predmet postupka, 6. datum donošenja rješenja ili naloga (čl. 168. st. 2. ZKP-a).

[16] izvor podataka: dopis Ravnateljstva policije, broj: 511-01-43-152-23/16 od 8. ožujka 2016.

skih mreža i usluga (čl. 1. Zakona), te definira temeljne pojmove elektroničke komunikacije: adresa, elektronička komunikacijska mreža, elektroničke komunikacije, javna komunikacijska mreža, javno dostupna telefonska usluga, komunikacija, korisnik usluga, operator, podaci o lokaciji, poziv i privola (čl. 2. Zakona).

III. DIREKTIVA 2006/24/EZ

Glavni cilj Direktive Europskog parlamenta i vijeća 2006/24/EZ od 15. ožujka 2006. o zadržavanju podataka proizvedenih ili obrađenih u vezi s pružanjem javnodostupnih elektroničkih komunikacijskih usluga ili javnih komunikacijskih mreža te o dopuni Direktive 2002/58/EZ je harmonizacija odredbi država članica koje se odnose na prikupljanje određenih podataka koji nastaju i koji se obrađuju od strane pružatelja usluga javnodostupnih elektroničkih komunikacijskih usluga i javnih komunikacijskih mreža. Direktivom se traži da se osigura dostupnost podataka u svrhu prevencije, istrage, otkrivanja i progona teških (ozbiljnih) kaznenih djela, posebice, organiziranog kriminala i terorizma. Dakle, Direktiva propisuje da spomenuti pružatelji usluga moraju prikupljati podatke o prometu i lokacijama, kao i podatke vezane za prepoznavanje pretplatnika ili korisnika. Za razliku od toga, Direktiva ne dopušta prikupljanje podataka o sadržaju komunikacije ili o informacijama koje su konzultirane putem komunikacije (navod 21. u preambuli i čl. 1.-2. Direktive).

Visoki sud Irske i Ustavni sud Austrije, rješavajući po tužbi tvrtke Digital Rights odnosno prema zahtjevu Vlade pokrajine Koruške i potpisnika zahtjeva da se preispita zakonitost nacionalnih zakona koji direktivu implementiraju u nacionalne propise Irske odnosno Austrije, obratili su se Europskom sudu (dalje ES), zahtjevom za prethodno mišljenje na temelju članka 267. Ugovora o funkcioniranju Europske unije (2010/C/ 083/01)[17], tražeći da ES ispita valjanost Direktive, posebice u svjetlu dvaju temeljnih prava iz Povelje o temeljnim pravima Europske unije (2010/C 083/02): prava na poštovanje privatnog i obiteljskog života[18] i prava na zaštitu osobnih podataka[19].

Presudom, u spojenim predmetima C-293/12 i C-594/12, Veliko vijeće ES-a je Direktivu proglasio nevaljanom.

ES je utvrdio da podaci koji se prikupljaju omogućavaju, posebice: 1. da se zna identitet osobe s kojom je pretplatnik ili registrirani korisnik komunicirao i na koji način, 2. da

[17] "Sud Europske unije je nadležan odlučivati o prethodnim pitanjima koja se tiču: a) tumačenja Ugovora, b) valjanosti i tumačenja akata institucija, tijela, ureda ili agencija Unije. Ako se takvo pitanje pojavi pred bilo kojim sudom države članice, taj sud može, ako smatra da je odluka o tom pitanju potrebna da bi mogao donijeti presudu, zatražiti od Suda da o tome odluči. Ako se takvo pitanje pojavi u predmetu koji je u tijeku pred sudom neke države članice, protiv čijih odluka prema nacionalnom pravu nema pravnog lijeka, taj je sud dužan uputiti to pitanje Sudu.", čl. 267. st.1.-3. Ugovora o funkcioniranju Europske unije.

[18] "Svatko ima pravo na poštovanje svog privatnog i obiteljskog života, doma i komunikacije.", čl. 7. Povelje o temeljnim pravima Europske unije.

[19] "Svatko ima pravo na zaštitu svojih osobnih podataka. Takvi podaci moraju se obrađivati pošteno u za to predviđene svrhe, na temelju pristanka osobe o kojoj je riječ ili na nekoj drugoj legitimnoj osnovi, utvrđenoj zakonom. Svatko ima pravo na pristup prikupljenim podacima koji se na njega ili na nju odnose i pravo na njihovo ispravljanje. Poštovanje tih pravila podliježe nadzoru neovisnog tijela.", čl. 8. st. 1.-3. Povelje o temeljnim pravima Europske unije.

se identificiraju vremena komunikacije i mjesto odakle je komunikacija uspostavljena i 3. da se može odrediti učestalost komunikacija pretplatnika ili registriranog korisnika s određenim osobama tijekom određenog razdoblja. Ti podaci, gledano u cjelini, mogu dati vrlo precizne informacije o privatnim životima osoba čiji se podaci prikupljaju, kao što su navike svakodnevnog života, podaci o stalnim ili privremenim mjestima prebivališta, svakodnevnim ili drugim kretanjima, aktivnostima koje osobe provode, društvenim odnosima i društvenom okruženju u kojem se osoba kreće. ES smatra da zahtjev za prikupljanje tih podataka i dopuštanje nadležnim tijelima državne vlasti za pristup tim podacima, predstavlja neposredno zadiranje na osobito ozbiljan način u temeljna prava na poštovanje privatnosti i zaštitu osobnih podataka. Činjenica da se ti podaci prikupljaju i kasnije koriste, a da se o tome ne obavijesti pretplatnik ili registrirani korisnik, dovodi do vjerojatnosti da će se kod osoba pojaviti osjećaj kako se njihovi privatni životi nalaze pod stalnim nadzorom (t. 26.-29.).

ES je ustanovio da se za prikupljanje podataka, na način kako je određeno Direktivom, ne može smatrati da ima učinak kojim se ide protiv smisla temeljnih prava na poštovanje privatnosti i zaštite podataka. Direktiva ne dopušta stjecanje znanja o sadržaju elektroničkih komunikacija kao takvih i osigurava da pružatelji usluga službi i mreža moraju poštovati određena načela zaštite podataka i sigurnosti podataka (t. 39.-40.) .

Nadalje, ES je zauzeo stajalište da prikupljanje podataka u svrhu njihovog mogućeg prijenosa nadležnim državnim tijelima vlasti u suštini zadovoljava cilj od općeg interesa, a to su borba protiv ozbiljnih oblika kriminala i, u konačnici, javna sigurnost (t. 41.)[20] .

Međutim, ES je iskazao mišljenje da je, usvajanjem Direktive 2006/24/EZ od 15. 3. 2006., zakonodavstvo Europske unije prekoračilo granice nametnute u skladu s načelom proporcionalnosti. Zaključak ES-a je Direktiva, unatoč tome što se prikupljanje podataka određeno Direktivom može smatrati prikladnim za postizanje cilja zbog kojeg je Direktiva donesena (t. 49. presude), imajući u vidu široki opseg i osobito ozbiljno zadiranje same Direktive u spomenuta temeljna prava, nije dovoljno uređena na način da se osigura da to zadiranje bude ograničeno na samo ono što je stvarno nužno (t. 65. i 69.):

---

[20] " 41. Što se tiče pitanja da li ovakvo zadiranje zadovoljava ciljeve od općeg interesa potrebno je naglasiti da unatoč tome što Direktiva 2006/24 cilja na harmonizaciju propisa država članica koji se odnose na obvezu pružatelja usluga na zadržavanje određenih podataka koji su nastali ili obrađeni od strane istih, materijalni cilj te direktive navodi se u članku 1(1) koji govori o potrebi da ti podaci budu na raspolaganju za potrebe istrage, otkrivanja i progona ozbiljnih oblika kriminala, kako je to definirano nacionalnim propisima država članica. Materijalni cilj ove Direktive je stoga doprinos borbi protiv ozbiljnih oblika kriminala, a samim time i javnoj sigurnosti. 42. Iz sudske prakse Suda očito je da je borba protiv međunarodnog terorizma, kako bi se održali međunarodni mir i sigurnost, predstavlja cilj od općeg interesa (vidi u tom smislu, predmeti C-402/05 P i C-415 / 05 P *Kadi i Al Barakaat International Fundation protiv Vijeća i Komisije EU*:C:2008:461, stavak 363., i predmeti C-539/10 P i C-550/10 P *Al-Aqsa protiv Vijeća EU*:C:2012:711, stavak 130.). Isto vrijedi i za borbu protiv ozbiljnih oblika kriminala, kako bi se osigurala javna sigurnost (vidi u tom smislu predmet C-145/09 *Tsakouridis protiv EU*:C:2010:708, stavci 46. i 47.). Nadalje, valja istaknuti u tom smislu, da članak 6. Povelje propisuje pravo bilo koje osobe ne samo na slobodu, već i na sigurnost. 43. U tom pogledu, razvidno je iz navoda 7 u preambuli Direktive 2006/24 da je, zbog značajnog rasta u mogućnostima koje pružaju elektroničke komunikacije, Vijeće za pravosuđe i unutarnje poslove dana 19. prosinca 2002. donijelo zaključak da su podaci koji se odnose na uporabu elektroničkih komunikacija posebno važni i stoga vrijedan alat u prevenciji kaznenih djela i borbi protiv kriminala, osobito organiziranog kriminala. 44. Stoga se mora zaključiti da zadržavanje podataka za potrebe omogućavanja nadležnim nacionalnim tijelima vlasti pristupa tim podacima, kako je propisano Direktivom 2006/24, uistinu zadovoljava cilj od općeg interesa."

Prvo, Direktiva se odnosi na sve osobe i na sva sredstva elektroničke komunikacije, kao i na sve podatke o prometu, bez ikakve razlike, ograničenja ili iznimke u pogledu ciljeva borbe protiv teškog kriminala (t. 57.)[21] .

Drugo, Direktiva nije postavila nikakve objektivne kriterije koji bi osigurali da nadležna nacionalna tijela vlasti imaju pristup podacima i da ih mogu koristiti samo u svrhu prevencije, otkrivanja i kaznenog progona vezanih za kaznena djela koja se, s obzirom na opseg i ozbiljnost zadiranja u predmetna temeljna prava, mogu smatrati dovoljno ozbiljnim da opravdaju takva zadiranja. Naprotiv, Direktiva se jednostavno poziva na općeniti pojam "ozbiljan kriminal" u smislu kako je to definirala svaka država članica u svojim nacionalnim zakonodavstvima. Također, Direktiva ne propisuje materijalne i proceduralne uvjete pod kojima nadležna državna tijela vlasti mogu imati pristup tim podacima i pravo na njihovo naknadno korištenje. Štoviše, pristup podacima i njihovo korištenje nije podložno prethodnoj kontroli odnosno odobrenju od suda ili neovisnog tijela uprave (t. 60.-62.) .

Treće, što se tiče razdoblja čuvanja podataka, Direktiva propisuje rok od najmanje šest mjeseci, a da se pri tom ne pravi nikakva razlika između kategorija podataka i kategorija osoba nad kojima se vrši prikupljanje podataka ili eventualne korisnosti podataka u odnosu postavljene ciljeve. Razdoblje čuvanja podataka je određeno između najmanje šest mjeseci, a najviše 24 mjeseca, a da se pri tom ne navode objektivni kriteriji na temelju kojih bi se odredilo razdoblje čuvanje podataka, kako bi se osiguralo da je čuvanje podataka ograničeno na ono razdoblje koje je prijeko potrebno (t. 63.-64.). ES smatra i da Direktiva nije propisala odredbe koje govore o razini dostatne zaštite kako bi se osigurala učinkovita zaštita podataka protiv rizika od zlouporabe i nezakonitog pristupa i korištenja podataka. Primjećuje se, između ostalog, da Direktiva dopušta pružateljima usluga da imaju u vidu kriterije ekonomske isplativosti prilikom određivanja razine sigurnosti koja se primjenjuje, posebno što se tiče troškova provedbe sigurnosnih mjera (t. 66.-67.). Također, ES konstatira da Direktiva ne zahtijeva da podaci budu zadržani na području EU-a, čime se ne zadovoljava u potpunosti kontrola usklađenosti sa zahtjevima zaštite i sigurnosti od strane neovisnog tijela, kao što to izrijekom zahtijeva Povelja (čl. 8. st. 3.), a navedena kontrola, koja se provodi na temelju prava EU, važna je komponenta zaštite pojedinaca s obzirom na obradu osobnih podataka (t. 68.).

[21] "58. Direktiva 2006/24 u širem smislu utječe na sve osobe koje koriste usluge elektroničke komunikacije, bez obzira da li se osoba čiji podaci se zadržavaju makar i indirektno nalazi u položaju koji bi davao razlog za kazneni progon. (…) Nadalje, ona ne određuje nikakve iznimke, što ima za rezultat da se primjenjuje čak i na osobe čija komunikacija je podložna, sukladno nacionalnom pravu, obvezi profesionalne tajnosti. 59. Štoviše, istovremeno dok proklamira doprinos borbi protiv ozbiljnih oblika kriminala, Direktiva 2006/24 ne zahtijeva nikakav odnos između podataka koji se zadržavaju i prijetnje javnoj sigurnosti (…)."

IV. ZAKLJUČAK

Provjera uspostavljenih telekomunikacijskih kontakata je neophodan alat u radu tijela koja istražuju kriminalne aktivnosti[22]. Svrha policijske ovlasti provjere uspostavljanja elektroničke komunikacije jest sprječavanje i otkrivanje kaznenih djela za koja se progoni po službenoj dužnosti i njihovih počinitelja, sprječavanje opasnosti i nasilja, te traganje za osobama i predmetima. Svrha dokazne radnje provjere uspostavljanja telekomunikacijskog kontakta jest prikupljanje dokaza radi kaznenog progona počinitelja težih kaznenih djela.

Odluka ES-a ne spori potrebu i opravdanost prikupljanja i obrade takvih podataka, no upozorava na povredu načela razmjernosti u odnosu na članke 7. 8. i 52. stavak 1. Povelje[23]. S obzirom na to da je ES Direktivu proglasio nevaljanom, precizirajući njezine nedostatke, zakonodavac će morati čim prije donijeti novu (poboljšanu) Direktivu, što utječe i na nacionalna zakonodavstva država članica, uključujući i Republiku Hrvatsku[24], a time i na ovlasti i rad tijela kaznenog progona.

Republika Hrvatska je, respektirajući stajališta ES-a, a pozivajući se i na potrebu usklađivanja zakonodavstva s Poveljom o temeljnim pravima Europske unije, novelirala zakonske odredbe koje reguliraju provjeru uspostavljanja telekomunikacijskih kontakata.

Treba istaknuti da je izmjenom odredbi o provjeri uspostavljanja telekomunikacijskih kontakata u ZKP-u, Republika Hrvatska upravo na propisan i dozvoljen način omogućila ograničenje prava na poštovanje privatnog i obiteljskog života iz članka 7. Povelje o temeljnim pravima Europske unije, ali i članka 8. Europske konvencije za zaštitu ljudskih prava i temeljnih sloboda, NN – MU 18/97., 6/99., 8/99., 14/02., 1/06.[25] Izmjenama u članku 339.a stavak 1. i 2. ZKP-a mogućnost provođenja dokazne radnje provjere uspostavljanja telekomunikacijskog kontakta dodatno je sužena i to na način da se ova dokazna radnja može

---

[22] Kralj (2009: 171) prikazao je komparativni zakonodavni okvir za 7 europskih država iz kojeg je vidljiva neupitna ovlast policije za provjeru uspostavljanja telekomunikacijskih kontakata, uz razliku je li u tu svrhu potrebno ishoditi nalog suda ili ne.

[23] "Svako ograničenje pri ostvarivanju prava i sloboda priznatih ovom Poveljom mora biti predviđeno zakonom i mora poštovati bit tih prava i sloboda. Uz poštovanje načela proporcionalnosti, ograničenja su moguća samo ako su potrebna i ako zaista odgovaraju ciljevima od općeg interesa koje priznaje Unija ili potrebi zaštite prava i sloboda drugih.", čl. 52. st.1. Povelje o temeljnim pravima Europske unije.

[24] Koliko je ova odluka ES-a šokirala ljude koji provode zakon najbolje govori izjava glasnogovornika britanske Vlade koji je izjavio da je korištenje ovih podataka bilo "od fundamentalnog značaja u cilju istraživanja kriminala i očuvanja nacionalne sigurnosti" te se ne smije dozvoliti situacija u kojoj prikupljanje podataka na neki način neće biti moguće. S druge strane, predstavnica Europske komisije je izjavila kako je u postupku procjena učinka same presude te kako će se osigurati "pravilna ravnoteža između sigurnosti i ljudskih prava." (izvor: https://www.bbc.com/news/world-europe-26935096).

[25] "Svatko ima pravo na poštovanje svoga privatnog i obiteljskog života, doma i dopisivanja. Javna vlast se neće miješati u ostvarivanje tog prava, osim u skladu sa zakonom i ako je u demokratskom društvu nužno radi interesa državne sigurnosti, javnog reda i mira, ili gospodarske dobrobiti zemlje, te radi sprječavanja nereda ili zločina, radi zaštite zdravlja ili morala ili radi zaštite prava i sloboda drugih.", čl. 8. st. 1.-2. Europske konvencije za zaštitu ljudskih prava i temeljnih sloboda.; Praksa Europskog suda za ljudska prava upućuje da "nadzor samo vanjskih obilježja tehničke komunikacije (kontakta telekomunikacijskih adresa), poput broja koji je biran s određene telefonske linije, vrijeme i duljine razgovora, također predstavlja zahvat za koji je nužna legitimacija prema stavku 2. *(Malone v. the United Kingdom)*"., Pavišić, 2006., str. 114.; O zahtjevima Europskog suda za ljudska prava za postojanje učinkovitih sredstava protiv arbitrarnog miješanja u konvencijska prava, vidi detaljnije u Omejec, 2013: 1114.-1116.

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 ove dokazne radnje u privatnost osobe prema kojoj se ona provodi, bilo je potrebno ograničiti mogućnost pristupa ovim podacima i njihovu naknadnu uporabu samo na teška kaznena djela kod kojih se takvo zadiranje može opravdati[26]. Izmjene članka 339.a Zakona o kaznenom postupku bile su nužne i radi usklađenja s Uredbom o obvezama iz područja nacionalne sigurnosti Republike Hrvatske za pravne i fizičke osobe u telekomunikacijama, NN 64/08., 76/13., kojom se propisuje i uloga Operativno-tehničkog centra za nadzor telekomunikacija prilikom provođenja mjera tajnog nadzora telekomunikacijskog prometa, pa je sada propisano da će policija (na temelju naloga suca istrage) provjeru istovjetnosti, trajanja i učestalosti komunikacije s određenim komunikacijskim adresama, utvrđivanje položaja komunikacijskog uređaja, kao i utvrđivanje mjesta na kojima se nalaze osobe koje uspostavljaju elektroničku komunikaciju te identifikacijske oznake uređaja od operatora javnih komunikacijskih usluga zatražiti putem Operativno-tehničkog centra za nadzor telekomunikacija.

LITERATURA

1. *Direktiva 2002/58/EZ.* (SL L 201, 31. 7. 2002.)
2. *Direktiva 2006/24/EZ.* (SL L 105, 13. 4. 2006.)
3. Dopis Ministarstva unutarnjih poslova Republike Hrvatske, Ravnateljstva policije, broj: 511-01-43-152-23/16 od 8. ožujka 2016.
4. *Europska konvencije za zaštitu ljudskih prava i temeljnih sloboda.* (NN – MU 18/97., 6/99., 8/99., 14/02., 1/06.)
5. https://www.bbc.com/news/world-europe-26935096
6. *Javni poziv za podnošenje prijedloga za imenovanje predsjednika i šest članova Vijeća za građanski nadzor sigurnosno-obavještajnih agencija.* (NN 17/16.)
7. Kralj, T. (2009). *Provjera istovjetnosti telekomunikacijskih adresa*. Policija i sigurnost, broj 2, Ministarstvo unutarnjih poslova, Zagreb.
8. Krapac, D. (2002). *Zakon o kaznenom postupku i drugi izvori hrvatskog postupovnog prava.* 4. izdanje, Narodne novine, Zagreb.
9. *Obrazloženje Prijedloga zakona o izmjenama i dopunama Zakona o kaznenom*

[26] "(…) valja imati u vidu da članci 7. i 8. Povelje o temeljnim pravima Europske unije 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 ovom izmjenom članka 339. a ZKP/08 i osigurava. Na obvezu poštivanja gore citiranih odredaba Povelje o temeljnim pravima Europske unije upozorio je i Sud Europske unije u svojoj presudi od 8. travnja 2014.u spojenim predmetima C-293/12 i C-594/12, kojom je nevaljanom proglašena Direktiva 2006/24/EZ od 15. ožujka 2006. o zadržavanju podataka dobivenih ili obrađenih u vezi s pružanjem javno dostupnih elektroničkih komunikacijskih mreža.", 4. Obrazloženje Prijedloga zakona o izmjenama i dopunama Zakona o kaznenom postupku, s konačnim Prijedlogom zakona, https://vlada.gov.hr/UserDocsImages//Sjednice/2014/189%20sjednica%20Vlade//189%20-%209.pdf

postupku. PZE 488, http://www.sabor.hr/prijedlog-zakona-o-izmjenama-i-dopunama-zakona-o-k

10. *Obrazloženje Prijedloga zakona o izmjenama i dopunama Zakona o kaznenom postupku s konačnim Prijedlogom zakona.*

    https://vlada.gov.hr/UserDocsImages//Sjednice/2014/189%20sjednica%20Vlade//189%20-%209.pdf
11. Odluka Europskog suda od 8. 4. 2014., u spojenim predmetima C-293/12 i C-594/12, http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d0f130d6ec5777fd78fb43099fc2c2f4cc0925b1.e34KaxiLc3eQc40LaxqMbN4OaNiRe0?text=&docid=150642&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=87158
12. Omejec, J. (2013). *Konvencija za zaštitu ljudskih prava i temeljnih sloboda u praksi Europskog suda za ljudska prava.* Novi informator, Zagreb.
13. Pavišić, B. (2006). *Kazneno pravo Vijeća Europe.* Golden marketing – Tehnička knjiga, Zagreb.
14. Pavišić, B. (2005). *Komentar Zakona o kaznenom postupku*. 5. izdanje, Žagar, Rijeka.
15. Pavišić, B. (2015). *Komentar Zakona o kaznenom postupku s prilozima.* Templar-book, Šmrika.
16. *Povelja o temeljnim pravima Europske unije* (2010/C 083/02).
17. *Pravilnik o načinu policijskog postupanja.* (NN 89/10., 78/14., 76/15.)
18. Standardni operativni postupak za djelovanje jedinstvenog operativno-komunikacijskog centra (Centra 112) kod dostave podataka o lokaciji korisnika za pozive iz mreža pokretnih telekomunikacija,

    http://www.duzs.hr/page.aspx?PageID=608
19. Tomašević, G., Krapac, D., Gluščić, S. (2005). *Kazneno procesno pravo.* Udžbenik za visoke škole. Narodne novine, Zagreb.
20. *Ugovor o funkcioniranju Europske unije* (2010/C/ 083/01).
21. *Uredba o obvezama iz područja nacionalne sigurnosti Republike Hrvatske za pravne i fizičke osobe u telekomunikacijama.* (NN 64/08., 76/13.)
22. Veić, P., Borovec, K., Brincki, Ž., Dundović, D., Kralj, T., Kovač, M., Ničeno, Z., Radmilović, Ž. (2009). *Zakon o policijskim poslovima i ovlastima.* Narodne novine, Zagreb.
23. *Zakon o elektroničkim komunikacijama.* (NN 73/08., 90/11., 133/12., 80/13., 71/14.)
24. *Zakon o kaznenom postupku.* (NN 110/97., 27/98., 58/99., 112/99.)
25. *Zakon o kaznenom postupku.* (NN 152/08., 76/09., 80/11., 121/11., 91/12., 143/12., 56/13., 145/13., 152/14.)
26. *Zakon o policijskim poslovima i ovlastima.* (NN 76/09., 92/14.)
27. *Zakon o sigurnosno-obavještajnom sustavu.* (NN 79/06., 105/06.)

Summary

Damir Juras, Antonio Vulas

Legal Framework for Checking of Telecommunication Contacts

This article gives an overview of the propositions which regulate processing and using of data generated by electronic communication, in particular the electronic communication data necessary for prevention and detection of the most serious types of crime. Specific attention has been given to the overview of the Judgement of the European Court of Justice in Luxemburg, which invalidates the Directive which regulates the field of generating and processing of telecommunication data. The article emphasises the fact that the Republic of Croatia has legally regulated field of checking of telecommunication contacts, by introducing some novelties in its legal system, in accordance with the directions of the European Court of Justice when it points out Directive's inconsistency with the fundamental rights on privacy and protection of the personal data.

Key words: Directive 2006/24/EC, European court of Justice, telecommunication control, Police, telecommunication contacts check.