UDK 343.985(497.11); 351.746.2(497.11)

CERIF: S 149

DOI: 10.51204/Anali_PFBU_25104A

Dr Milana M. PISARIĆ[*]

Ostoja S. KALABA, master[**]

ZADRŽAVANJE PODATAKA I KRIVIČNI POSTUPAK U SRBIJI[***]

Upotreba informacione tehnologije omogućava nadležnim državnim organima da prilikom preduzimanja mera i radnji radi sprečavanja, otkrivanja i istrage krivičnih dela te krivičnog gonjenja učinilaca krivičnih dela obrađuju podatke o ličnosti u do sada nezabeleženom obimu i na nezamisliv način. Jedna od spornih obrada je ostvarivanje masovnog, neselektivnog nadzora elektronskih komunikacija u vidu zadržavanja komunikacionih podataka, koji o pojedincu ponekad mogu da otkriju više i od samog sadržaja komunikacije. Takva obrada podataka predstavlja mešanje u garantovana ljudska prava i slobode, a da to ne bi bilo i njihovo kršenje, morala bi da bude pravno uređena u skladu sa Ustavom i međunarodnim standardima zaštite ljudskih prava. Autori u radu analiziraju pravni okvir za zadržavanje komunikacionih podataka i pristup zadržanim podacima za potrebe krivičnog postupka u Srbiji, posebno u svetlu relevantne prakse Suda pravde Evropske unije i Evropskog suda za ljudska prava.

Ključne reči: *Elektronske komunikacije. – Zadržavanje podataka. – Krivični postupak. – Zaštita podataka o ličnosti. – Privatnost.*

---

[*] Docentkinja, Univerzitet u Novom Sadu – Pravni fakultet, Srbija, *mpisaric@pf.uns.ac.rs*, ORCID iD: 0000–0001–8344–3349.

[**] Savetnik u Službi Poverenika za informacije od javnog značaja i zaštitu podataka o ličnosti, doktorand, Srbija, *kalaba.ostoja@gmail.com*.

[***] Pojedini delovi istraživanja bili su izloženi u vidu usmenog saopštenja na temu „Data retention and access to retained data for the purpose of criminal procedure in Serbia", na naučnom skupu *SSN2024: Surveillance in an Age of Crisis: the 10th Biennial Surveillance Studies Network / Surveillance & Society Conference 2024, hosted by the Institute of Criminology at the Faculty of Law and the Faculty of Law, University of Ljubljana, Slovenia*, održanom od 28. do 31. maja 2024. godine na Pravnom fakultetu Univerziteta u Ljubljani.

1. UVOD

Kada je Edvard Snouden otkrio da je *NSA* masovno prikupljala određene metapodatke o komunikacijama, veliki deo sveta bio je šokiran i iznenađen. Iako je tadašnji predsednik Sjedinjenih Američkih Država (SAD) u svom govoru početkom 2014. godine izjavio da se takvim sistemom ne prikupljaju sadržaj telefonskih poziva ni imena lica koja razgovaraju (*Washington Post*, 2014), akademska i stručna javnost je razumela i ono što nije rečeno – da je reč o masovnom prikupljanju metapodataka, te da takav nadzor predstavlja zadiranje u privatnost, a bez odgovarajućih, strogih kriterijuma za primenu i bez efektivne kontrole od nezavisnih nadzornih organa, potencijalno i kršenje pojedinih osnovnih ljudskih prava i sloboda, te da vodi ka orvelovskom društvu.[1] Takva „praksa" nije bila ni u tom trenutku, a ni sada, svojstvena samo SAD – već godinama je opravdano predmet rasprave u javnom i naučnom diskursu[2], (neadekvatne) regulative i posledično sudskog preispitivanja u mnogim državama.

Pravo Evropske unije (EU) uticalo je na pravno uređenje elektronskih komunikacija u Srbiji, pa i u pogledu zadržavanja komunikacionih podataka i pristupa tim podacima. Usvajanjem Direktive o zadržavanju podataka[3] (Direktiva 2006/24/*EC*) na nivou EU je stvorena obaveza pružalaca javno dostupnih usluga elektronske komunikacije ili javnih komunikacionih mreža da zadrže određene podatke koje prikupljaju ili obrađuju u vezi sa tim uslugama, kako bi se osiguralo da budu dostupni nadležnim organima u svrhu otkrivanja i dokazivanja teških krivičnih dela te otkrivanja i krivičnog gonjenja učinilaca tih dela. Međutim, srpski zakonodavac nije u dovoljnoj meri i na odgovarajući način ispratio dalju sudbinu Direktive 2006/24/*EC* i propisa o zadržavanju podataka u državama članicama, naročito s obzirom na odluke

[1] Više o tome Pisarić (2019, 156).

[2] Više o tome npr. Rojszczak, Marcin. 2021. National Security and Retention of Telecommunications Data in Light of Recent Case Law of the European Courts, *European Constitutional Law Review* 17(4): 607–635 i Rojszczak, Marcin. 2021. The uncertain future of data retention laws in the EU: Is a legislative reset possible? *Computer Law & Security Review* 41, July.

[3] Directive 2006/24/EC of The European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ L 105/54 of 13/4/2006.

Suda pravde EU. Osim toga, nisu uzete u obzir ni relevantne odluke Evropskog suda za ljudska prava (ESLJP), u kojima je utvrđeno kršenje prava iz Evropske konvencije o ljudskih pravima (EKLJP) u vezi sa zadržavanjem podataka. Autori u ovom radu analiziraju domaći pravni okvir zadržavanja podataka i pristupa nadležnih organa zadržanim podacima za potrebe krivičnog postupka, koji sagledavaju posebno kroz prizmu odluka Suda pravde EU i ESLJP.

2. PRAVNI OKVIR U SRBIJI

U Srbiji je, po uzoru na Direktivu 2006/24/*EC*, zadržavanje podataka o elektronskim komunikacijama normirano 2010. godine usvajanjem Zakona o elektronskim komunikacijama,[4] u glavi XVII „Tajnost elektronskih komunikacija, zakonito presretanje i zadržavanje podataka". Pojedine odredbe iz te glave proglašene su neustavnim 2013. godine Odlukom Ustavnog suda Republike Srbije[5] (Odluka US), a pojedine su izmenjene sledeće godine.[6] Nakon tih intervencija, odredbe iz glave XVII i dalje važe, iako je 2023. godine usvojen novi Zakon o elektronskim komunikacijama[7] (ZEK 2023). Naime, u čl. 180 st. 1 ZEK 2023 propisano je da stupanjem na snagu tog zakona prestaje da važi prethodni Zakon o elektronskim komunikacijama[8] (ZEK), a istovremeno je utvrđeno, iz neobjašnjivih i legislativno neopravdanih razloga, da su i dalje na snazi pojedine odredbe ZEK, među kojima su upravo odredbe o zadržavanju podataka. Budući da je propušteno (ili izbegnuto) da se u novom propisu kojim se uređuju elektronske komunikacije normira i zadržavanje podataka, relevantne odredbe su neprirodno i nepregledno ostale van organskog teksta sistemskog zakona. Radi sveobuhvatnog sagledavanja pravnog okvira zadržavanja podataka, važno je napomenuti da su načelna pravila sadržana u nekoliko članova ZEK i da su bliže uređena podzakonskim aktima (usvojenim na osnovu zakona koji je prestao da važi). U nastavku ćemo analizirati zadržavanje podataka i pristup zadržanim podacima kao dva koraka jednog mehanizma.

---

4 *Službeni glasnik RS* 44/10.

5 Ustavni sud Republike Srbije, Iuz 1245/2010, 13. jun 2013, *Službeni glasnik RS* 60/13, 74–80.

6 Zakon o izmenama i dopunama Zakona o elektronskim komunikacijama, *Službeni glasnik RS* 62/2014.

7 *Službeni glasnik RS* 35/23.

8 *Službeni glasnik RS* 44/10, 60/13 – odluka US, 62/14, 95/18 – dr. zakon i 35/23 – dr. zakon.

1.1. Zadržavanje podataka

1.1.1. Svrha zadržavanja

U čl. 128 st. 1 izvornog teksta ZEK bilo je predviđeno da je operator *dužan da zadrži* podatke o elektronskim komunikacijama za potrebe sprovođenja istrage, otkrivanja krivičnih dela i vođenja krivičnog postupka, u skladu sa zakonom kojim se uređuje krivični postupak, te za potrebe zaštite nacionalne i javne bezbednosti Republike Srbije, *u skladu sa zakonima kojima se uređuje rad službi bezbednosti Republike Srbije i rad organa unutrašnjih poslova*. Deo odredbe kojim se upućuje na te druge zakone proglašen je 2013. godine *neustavnim* Odlukom US.[9] Naredne godine čl. 128 je *izmenjen*, tako što je potpuno *izostavljena svrha zadržavanja podataka*. Trenutno važeći ZEK prosto propisuje dužnost operatora da zadrži podatke o elektronskim komunikacijama (čl. 128 st. 1) i da zadržane podatke čuva 12 meseci od dana obavljene komunikacije (čl. 128 st. 6), *ne određujući svrhu* zbog koje su te obaveze ustanovljene.

1.1.2. Podaci koji se zadržavaju

Što se tiče podataka u pogledu kojih postoje obaveze operatora, čl. 128 st. 1 ZEK upućuje na čl. 129 st. 1, koji utvrđuje *kategorije podataka* koji se zadržavaju *radi zadovoljenja određenih potreba*. Odgovor na pitanje *koji se to tačno podaci zadržavaju* daje podzakonski akt – Pravilnik o zahtevima za uređaje i programsku podršku za zakonito presretanje elektronskih komunikacija i tehničkim zahtevima za ispunjenje obaveze zadržavanja podataka o elektronskim komunikacijama[10] (Pravilnik[11]) – koji u čl. 11–16 *taksativno* propisuje koje

[9] Ustavni sud (US) je našao da deo „u skladu sa zakonom kojim se uređuje krivični postupak" i deo „u skladu sa zakonima kojima se uređuje rad službi bezbednosti Republike Srbije i rad organa unutrašnjih poslova" nisu u saglasnosti sa čl. 41 st. 2 Ustava, jer je jedino sud nadležan da dozvoli (odobri) odstupanje od Ustavom zajemčene nepovredivosti tajnosti pisama i drugih sredstava komuniciranja, „a ne da se to pravo određuje u skladu sa zakonom". Vid. Odluka US, 79.

[10] *Službeni glasnik RS* 88/2015.

[11] Izvorno, u čl. 129. st. 4 ZEK bilo je propisano da će *ministarstvo* nadležno za telekomunikacije, po pribavljenom mišljenju ministarstva nadležnog za poslove pravosuđa, ministarstva nadležnog za unutrašnje poslove, ministarstva nadležnog za poslove odbrane, Bezbednosno-informativne agencije i organa nadležnog za zaštitu podataka o ličnosti *bliže propisati zahteve u vezi sa zadržavanjem podataka* iz čl. 129 st. 1. Kada je US neustavnom proglasio odredbu čl. 128 st. 5, isto je učinio i sa čl. 129 st. 4 – čime je nestao pravni osnov za podzakonsko regulisanje obaveze zadržavanja podataka. Međutim, takav akt je ipak usvojen. Naime, čl. 127, kojim se

podatke su operatori dužni da zadrže. Zadržavaju se podaci koji su *potrebni za*: 1) praćenje i utvrđivanje *izvora* komunikacije,[12] 2) utvrđivanje *odredišta* komunikacije,[13] 3) utvrđivanje *početka, trajanja i završetka* komunikacije,[14]

inače uređuje zakonito presretanje elektronskih komunikacija, izmenjen je 2014. godine tako što je u st. 5 dodato da će ministarstvo bliže propisati *i tehničke zahteve za ispunjenje obaveze zadržavanja podataka* iz čl. 128 i 129 zakona. Pravilnik je usvojen upravo na osnovu te odredbe.

[12] Shodno čl. 11 Pravilnika, to su sledeći podaci: a) o javno dostupnoj telefonskoj usluzi na fiksnoj lokaciji i javno dostupnoj telefonskoj usluzi u javnoj mobilnoj komunikacionoj mreži: broj sa koga je inicirana komunikacija; ime i prezime fizičkog lica, odnosno naziv pravnog lica i adresa pretplatnika ili registrovanog korisnika; b) o internet pristupu, elektronskoj pošti, usluzi prenosa govora korišćenjem interneta i drugih oblika paketske razmene: dodeljeni korisnički identifikator ili telefonski broj za svaku komunikaciju u javnoj elektronskoj komunikacionoj mreži; ime i prezime fizičkog lica, odnosno naziv pravnog lica i adresu pretplatnika ili registrovanog korisnika kome je dodeljena *IP* adresa, korisnička identifikacija ili telefonski broj u vreme komunikacije; dinamička ili statička *IP* adresa dodeljena od provajdera usluge ili provajdera pristupa i korisnička identifikacija pretplatnika ili registrovanog korisnika; identifikacija digitalne pretplatničke linije ili druge tačke izvorišta komunikacije.

[13] Shodno čl. 12 Pravilnika, to su sledeći podaci: a) o javno dostupnoj telefonskoj usluzi na fiksnoj lokaciji i javno dostupnoj telefonskoj usluzi u javnoj mobilnoj komunikacionoj mreži: odabrani broj (broj koji je pozvan), a u slučaju dodatnih usluga (usmeravanje, prenošenje komunikacije i konferencijska veza) i broj na koji je komunikacija preusmerena, odnosno brojevi koji su uključeni u konferencijsku vezu; ime i prezime i adresa pretplatnika ili registrovanog korisnika; b) o internet pristupu, elektronske pošte, usluzi prenosa govora korišćenjem interneta i drugim oblicima paketske komunikacije: dinamička ili statička *IP* adresa dodeljena od provajdera usluge ili provajdera pristupa i korisnička identifikacija pretplatnika ili registrovanog korisnika u vreme komunikacije; korisnička identifikacija ili telefonski broj pripadajućeg sagovornika usluge prenosa govora korišćenjem interneta; ime i prezime i adresa pretplatnika ili registrovanog korisnika, kao i korisnička identifikacija pripadajućeg sagovornika u komunikaciji; identifikacija digitalne pretplatničke linije ili druge tačke odredišta komunikacije; podaci o komunikaciji (shodno čl. 2 st. 1 tač. 8 to su podaci koji predstavljaju signalizaciju povezanu s ciljanom elektronskom komunikacionom uslugom, mrežom ili drugim korisnikom, uključujući i signalizaciju upotrebljenu za uspostavljanje komunikacije, kontrolu njenog toka (npr. komunikacija prihvaćena, komunikacija prebačena), čija su sadržina i podaci dostupni operatorima elektronskih komunikacija (npr. vreme trajanja komunikacije).

[14] Shodno čl. 13 Pravilnika, to su sledeći podaci: a) o javno dostupnoj telefonskoj usluzi na fiksnoj lokaciji i javno dostupnoj telefonskoj usluzi u javnoj mobilnoj komunikacionoj mreži: datum, vreme početka, trajanja i završetka komunikacije; b) o internet pristupu, elektronskoj pošti, usluzi prenosa govora korišćenjem interneta i drugih oblika paketske komunikacije: datum, vreme prijave i odjave prilikom korišćenja pristupne usluge, u okviru odgovarajuće vremenske zone, kao

4) utvrđivanje *vrste* komunikacije,[15] 5) identifikaciju *terminalne opreme* korisnika[16] i 6) utvrđivanje *lokacije mobilne terminalne opreme korisnika*.[17] Osim toga, odredbama ZEK je propisano da obaveza zadržavanja obuhvata i podatke o uspostavljenim pozivima koji nisu odgovoreni, ali ne i podatke o pozivima čije uspostavljanje nije uspelo (čl. 129 st. 2), kao ni podatke koje operator nije proizveo niti obradio (čl. 129 st. 5). Izričito je zabranjeno zadržavanje podataka koji otkrivaju sadržaj komunikacije (čl. 129 st. 3).

i datum i vreme slanja i primanja elektronske pošte i poziva putem usluge prenosa govora korišćenjem interneta, u okviru odgovarajuće vremenske zone, za usluge koje pruža operator.

[15] Shodno čl. 14 Pravilnika, to su sledeći podaci: a) o javno dostupnoj telefonskoj usluzi na fiksnoj lokaciji i javno dostupnoj telefonskoj usluzi u javnoj mobilnoj komunikacionoj mreži: podaci o korišćenoj telefonskoj usluzi; b) o elektronskoj pošti, usluzi prenosa govora korišćenjem interneta i drugim oblicima paketske komunikacije: podaci o korišćenoj internet usluzi.

[16] Shodno čl. 15 Pravilnika, to su sledeći podaci: a) o javno dostupnoj telefonskoj usluzi u javnoj mobilnoj komunikacionoj mreži: *IMSI* broj sa kojeg je inicirana komunikacija i *IMSI* broj prema kojem je inicirana komunikacija, kao i *IMEI* broj sredstva za komuniciranje sa koga je inicirana komunikacija i *IMEI* broj prema kojem je inicirana komunikacija; b) o pripejd usluzi kod javno dostupne telefonske usluge na fiksnoj lokaciji i kod javno dostupne telefonske usluge u javnoj mobilnoj komunikacionoj mreži: serijski broj kartice (za javno dostupnu telefonsku uslugu na fiksnoj lokaciji) i serijski broj pripejd kartice i mesto sa koga je izvršena elektronska dopuna, ukoliko je to moguće za javno dostupnu telefonsku uslugu u javnoj mobilnoj komunikacionoj mreži; v) o pripejd usluzi kod internet pristupa, elektronskoj pošti, usluzi prenosa govora korišćenjem interneta i drugim oblicima paketske razmene: serijski broj kartice; g) o javno dostupnoj telefonskoj usluzi na fiksnoj lokaciji, internet pristupu, elektronskoj pošti, usluzi prenosa govora korišćenjem interneta i drugim oblicima paketske komunikacije: serijski broj uređaja, *MAC* adresa, dinamička i statička *IP* adresa dodeljena od provajdera usluge ili pristupa, u odgovarajućoj vremenskoj zoni, drugi podaci koji jednoznačno identifikuju terminalni uređaj korisnika.

[17] U čl. 16 Pravilnika nije određeno koji se to podaci zadržavaju nego je propisana dužnost operatora da omogući tehničko povezivanje svoje opreme sa opremom nadležnih državnih organa upotrebom odgovarajućeg tehničkog interfejsa kojim se omogućava prenos podataka o svim mobilnim terminalnim uređajima koji su se pojavili na određenoj geografskoj, fizičkoj ili logičkoj lokaciji, a u skladu sa tehničkim standardima ili mogućnostima pojedine mobilne elektronske komunikacione tehnologije.

1.2. Pristup zadržanim podacima

1.2.1. Svrha ostvarivanja pristupa

U izvornom tekstu ZEK nije bila predviđena svrha ostvarivanja pristupa zadržanim podacima, a nakon što je čl. 128 izmenjen 2014. godine, važećim ZEK je najpre propisano da pristup zadržanim podacima nije dopušten bez pristanka korisnika, a potom je takvu mogućnost predviđena *kao izuzetak* (čl. 128 st. 2). Naime, pristup zadržanim podacima je dopušten izuzetno „na određeno vreme i na osnovu odluke suda". Pri tome, odredbama ZEK je jasno određena *svrha* ostvarivanja pristupa zadržanim podacima, a to je neophodnost vođenja krivičnog postupka ili zaštite bezbednosti RS, [18] dok u pogledu načina upućuje na drugi zakon.

Propis kojim bi trebalo da se uredi ostvarivanje pristupa zadržanim podacima kada je to neophodno radi vođenja krivičnog postupka je Zakonik o krivičnom postupku[19] (ZKP). U čl. 286 („Ovlašćenja policije") ZKP propisana je *dužnost policije*, ukoliko postoje *osnovi sumnje* da je izvršeno *krivično delo* za koje se goni *po službenoj dužnosti*, da preduzme potrebne mere i radnje *sa ciljem* da se pronađe učinilac krivičnog dela, da se učinilac ili saučesnik ne sakrije ili ne pobegne, da se otkriju i obezbede tragovi krivičnog dela i predmeti koji mogu poslužiti kao dokaz te da se prikupe sva obaveštenja koja bi mogla biti od koristi za uspešno vođenje krivičnog postupka. Radi ispunjenja te dužnosti policija može, *po nalogu* sudije za prethodni postupak, a na predlog javnog tužioca da: 1) pribavi evidenciju (već) ostvarene *telefonske* komunikacije, 2) pribavi evidenciju korišćenih baznih stanica, 3) izvrši lociranje mesta „sa kojeg se obavlja komunikacija" (čl. 286 st. 3).

1.2.2. Način ostvarivanja pristupa

Operator je dužan da zadržava podatke na *način* da im se *bez odlaganja* može *pristupiti*, odnosno da se bez odlaganja mogu *dostaviti* na osnovu odluke suda (čl. 128 st. 7). Analizom ZEK i podzakonskih akata može se uočiti da nadležni državni organi dolaze do zadržanih podataka na dva

[18] U izvornom tekstu ZEK zakonodavac je bio odredio *zaštitu nacionalne i javne bezbednosti* Republike Srbije kao svrhu zadržavanja podataka (u čl. 128 st. 1, pre izmena), dok je prilikom formulisanja izmenjenog čl. 128 i određivanja svrhe pristupa zadržanim podacima (čl. 128 st. 2) dosledno ispratio tekst iz čl. 41. st. 2 Ustava (u kojem stoji „zaštita bezbednosti RS").

[19] *Službeni glasnik RS* 72/11, 101/11, 121/12, 32/13, 45/13, 55/14, 35/19, 27/21 – odluka US i 62/21 – odluka US.

načina: a) *neposredno* – tako što *ostvaruju pristup* prostorijama, elektronskoj komunikacionoj mreži, pripadajućim sredstvima ili elektronskoj komunikacionoj opremi operatora; ili b) *posredno* – tako što im operatori *dostavljaju tražene podatke.*[20]

Jasniji odgovor na pitanje šta se pod tim podrazumeva saznajemo iz Pravilnika. Pravilnik sadrži opštu odredbu kojom je propisano da *svi podaci* koji se zadržavaju u skladu sa ZEK moraju nadležnim državnim organima, *putem odgovarajućeg tehničkog interfejsa*, biti *dostupni* za period od poslednjih 12 meseci od dana obavljene komunikacije, a u skladu sa zakonom (čl. 9 st. 2 Pravilnika). U pogledu *podataka o lokaciji*, Pravilnik u čl. 16 i 21 obavezuje operatore da omoguće tehničko povezivanje svoje opreme sa opremom nadležnih državnih organa *upotrebom odgovarajućeg tehničkog interfejsa*, putem koga se omogućava *prenos* određenih komunikacionih podataka.[21]

1.3. Zadržavanje podataka, pristup zadržanim podacima i Ustav

Prilikom normiranja zadržavanja podataka nije u dovoljnoj meri i na adekvatan način sagledan jedan važan aspekt, a to je opravdanost takvog mešanja u garantovana ljudska prava i slobode. Odredbama ZEK se načelno predviđa, a podzakonskim aktima precizno uređuje zadržavanje velikog broja podataka, koji nadležnim organima, kada im pristupe i obrade ih, čak i kada se to vrši u legitimnom cilju, omogućuju donošenje vrlo preciznih zaključaka o privatnom životu lica čiji su podaci zadržani, kao što su svakodnevne navike, mesta trajnih ili privremenih boravaka, dnevna ili druga kretanja, obavljane aktivnosti, društveni odnosi i društvene sredine koje su lica posećivala – što sve ima značajan i potencijalno sveobuhvatan uticaj na pravo na privatnost i zaštitu podataka o ličnosti, kao i na pravo na slobodu izražavanja i kretanja.

[20] Jasno razlikovanje između dva režima pristupa zadržanim podacima proizlazi i iz obaveze vođenja evidencija (čl. 128 st. 8 i 9 ZEK, čl. 10 Pravilnika) i obaveze stvaranja tehničkog interfejsa posredstvom kojeg se zadržani podaci čine dostupnim nadležnim organima, kako se to Pravilnikom zahteva.

[21] Reč je o: a) podacima *o svim* mobilnim terminalnim *uređajima* koji su se pojavili na određenoj geografskoj, fizičkoj ili logičkoj lokaciji, shodno čl. 16 st. 1; b) podacima *o trenutnoj* geografskoj, fizičkoj ili logičkoj *lokaciji pojedinačnog sredstva* za elektronsku komunikaciju, shodno čl. 21 st. 1. Pravilnika.

S tim u vezi, neophodno je osvrnuti se na *usklađenost relevantnih odredaba* ZEK i ZKP sa *čl. 41* Ustava Republike Srbije[22] (Ustav) kojim se *garantuje nepovredivost tajnosti* pisama i drugih sredstava komuniciranja (st. 1), [23] a *odstupanje* dozvoljava samo na određeno vreme i na osnovu odluke suda, ako je to neophodno radi vođenja krivičnog postupka ili zaštite bezbednosti Republike Srbije, na način predviđen zakonom (st. 2).

U Odluci US je pre više od 10 godina istaknuto da *ustavnopravna zaštita obuhvata* ne samo sadržaj nego i *formalna obeležja komunikacije*,[24] što znači da i odstupanje od nepovredivosti tajnosti podataka o komunikaciji može biti dozvoljeno jedino ako je u skladu sa Ustavom.

Samo po sebi, sveopšte masovno zadržavanje i čuvanje podataka o svim komunikacijama svih korisnika na osnovu ZEK nesumnjivo predstavlja odstupanje od garantovane tajnosti komunikacija – a moglo bi biti dozvoljeno samo ako bi bili ispunjeni uslovi koji su propisani Ustavom. Ipak, čini se da zakonodavac zadržavanje podataka ne tretira kao odstupanje od ustavne garancije – ne određuje svrhu zbog koje su operatori dužni da zadrže i čuvaju podatke (neophodnost vođenja krivičnog postupka ili zaštite bezbednosti Republike Srbije). Svrha zadržavanja podataka ne može se izvoditi iz svrhe ostvarivanja pristupa zadržanim podacima, propisane u čl. 128 st. 2, jer su zadržavanje i pristup zadržanim podacima dva vida odstupanja od garantovanih prava i neophodno je posebno opravdanje za svaki. Takođe, navođenje određenih „potreba" zbog koje se pojedine kategorije podataka zadržavaju u čl. 129 st. 1 nije isto što i određivanje svrhe zadržavanja podataka. Osim toga, zahtevi da je odstupanje dozvoljeno „na osnovu odluke suda" i „na određeno vreme" nisu uzeti u obzir kada je propisana obaveza zadržavanja i čuvanja podataka.

Prilikom normiranja pristupa zadržanim podacima, zakonodavac se u čl. 128 st. 2 ZEK dosledno rukovodio formulacijom iz Ustava.[25] Međutim, ne bi se moglo reći da ZKP, kojim bi trebalo da se uredi odstupanje od garantovane

---

22 *Službeni glasnik RS* 98/06, 115/21 – amandmani I–XXIX i 16/22.

23 Interesantno je primetiti da i ZEK i ZEK 2023 sadrže pravilo o tajnosti komunikacija. Međutim, dok se u glavi XVII ZEK, u kojoj su odredbe o zadržavanju podataka, tajnost vezuje samo za sadržaj elektronskih komunikacija (čl. 126), u ZEK 2023 se jasno prepoznaje i tajnost i sa njima povezanih podataka o saobraćaju povezanih sa elektronskim komunikacijama (čl. 160 ZEK 2023).

24 Odluka US, 78.

25 Moguće je da je zakonodavac prilikom izmene čl. 128 uzeo u obzir i argumente iz Odluke US. Naime, Ustavni sud je našao da, iako je osporenom odredbom (izvornog čl. 128 st. 1) *propisana samo opšta obaveza* operatora da zadržava podatke i *određena svrha* zbog koje se zadržavanje propisuje *a ne i način korišćenja* zadržanih podataka, sporno je to što se *uvođenje te obaveze* vrši u skladu sa

nepovredivosti tajnosti komuniciranja radi vođenja krivičnog postupka, to čini na ispravan način, iz najmanje dva razloga: a) odstupanje može biti odobreno samo odlukom suda – a nalog nije odluka suda (ZKP poznaje tri vrste odluka u krivičnom postupku: naredbu, rešenje i presudu – čl. 269); b) odstupanje je dopušteno samo „na određeno vreme" – a u čl. 286 st. 3 ZKP takav zahtev se ne postavlja.

Takođe, ovlašćenje iz čl. 286 st. 3 ZKP odnosi se na pribavljanje *nekih od podataka koji se zadržavaju*, odnosno samo podataka o telefonskoj komunikaciji, ali ne i o ostalim vidovima elektronske komunikacije. Shodno tome, taj član *ne bi mogao da se koristi za ostvarivanje pristupa* svim onim kategorijama i vrstama podataka koji se zadržavaju na osnovu ZEK i Pravilnika, a koji nisu njime obuhvaćeni[26] – drugim rečima, odredbama ZKP se ne uređuje način na koji se njima ostvaruje pristup. Osim toga, zahtev za dostavljanje takvih zadržanih podataka, koji bi eventualno operatorima uputila policija ili javno tužilaštvo na osnovu opštih odredaba ZKP, bio bi sporan sa stanovišta ustavnosti.

Pitanjem ustavnosti odredaba o zadržavanju podataka bavio se i poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti (poverenik), kada je pre više od deset godina izvršio nadzor nad sprovođenjem i izvršavanjem Zakona o zaštiti podataka o ličnosti[27] (ZZPL) od strane rukovalaca-operatora mobilne i fiksne telefonije u Republici Srbiji (Izveštaji poverenika za 2012).[28]

---

drugim, odgovarajućim zakonima, na koji način se ustanovljava obaveza operatora *kojom posredno može doći do povrede tajnosti sredstava komunikacije* ukoliko se zadržani podaci ne koriste saglasno čl. 41 st. 2 Ustava, što znači bez odluke suda i bez određivanja vremena u kome se oni koriste *već na osnovu rešenja iz navedenih zakona*. Ustavni sud je istakao: „Uslovi i svrha dozvoljenog odstupanja od tajnosti sredstava komuniciranja su utvrđeni Ustavom i kao takvi ne mogu biti predmet zakonske materije, jer se način ostvarivanja ovog prava može propisati samo zakonom." Odluka US, 78.

[26] Primera radi, čl. 286 st. 3 ZKP se ne bi mogao primeniti za pribavljanje podatka o dinamičkoj ili statičkoj *IP* adresi dodeljenoj od provajdera usluge ili provajdera pristupa, koji se zadržava u smislu čl. 12 Pravilnika, ili podatka o datumu, vremenu prijave i odjave prilikom korišćenja pristupne usluge, u okviru odgovarajuće vremenske zone, kao i datumu i vremenu slanja i primanja elektronske pošte i poziva putem usluge prenosa govora korišćenjem interneta, u okviru odgovarajuće vremenske zone, za usluge koje pruža operator, koji se zadržava u smislu čl. 13 Pravilnika – čak i kada bi sud izdao nalog za pribavljanje takvih podataka.

[27] *Službeni glasnik RS* 87/18.

[28] Predmet nadzora je bio pristup zadržanim podacima o komunikaciji, pa je, na osnovu utvrđenih činjenica tokom nadzora, konstatovano da obrada tih podataka, svakog pojedinačno, a pogotovo svih zajedno, i to u periodu od 12 meseci, predstavlja ozbiljno zadiranje u privatnost građana, te da se time odstupa od ustavne

Na osnovu rezultata tog nadzora, poverenik i zaštitnik građana su u 14 tačaka pripremili Predlog preporuka za unapređenje stanja u ovoj oblasti, za koje se, uzimajući u obzir analizirano u ovom radu, ne može sa sigurnošću reći da su do današnjeg dana primenjene u punom i adekvatnom obimu. Slična je situacija i sa operatorima elektronskih komunikacija koji pružaju usluge pristupa internetu i internet usluge (Izveštaj poverenika za 2015).

Ne samo da je upitna usklađenost pravnog okvira o zadržavanju i pristupu zadržanim podacima sa Ustavom nego i usaglašenost s pravom EU i sa EKLJP jer se ne uzimaju u obzir standardi zaštite ljudskih prava utvrđeni u praksi Suda pravde EU i ESLJP.

3. STANDARDI ZAŠTITE LJUDSKIH PRAVA

3.1. Praksa Suda pravde EU

Iako je Direktiva 2006/24/*EC* još pre deset godina stavljena van snage jer je široko i osobito teško zadirala u osnovna ljudska prava, a da takvo mešanje nije bilo precizno ograničeno na ono što je strogo nužno,[29] komunikacioni podaci se i dalje zadržavaju u državama članicama, a nacionalni propisi i postupanje nadležnih organa u više država bili su predmet preispitivanja od Suda pravde EU.[30] Da bi se utvrdio stav Suda Pravde EU o zadržavanju podataka i pristupu zadržanim podacima od nadležnih organa u državama članicama, analizirane su odluke u predmetima *SpaceNet AG*,[31] *Tele2 Sverige*,[32] *La Quadrature du Net*,[33] *Privacy International*[34] i *Prokuratuur*.[35]

garancije nepovredivosti tajnosti sredstava komuniciranja i od odredbe da su odstupanja dozvoljena samo na određeno vreme i na osnovu odluke suda, radi vođenja krivičnog postupka ili zaštite državne bezbednosti.

29 CJEU, joined cases C-293/12 and C-594/12, 8 April 2014.

30 Više o tome Podkowik, Rybski, Zubik 2021, 1608–1609.

31 CJEU, joined cases C-793/19 and C-794/19, 27 October 2022.

32 CJEU, joined cases C-203/15 and C-698/15, 21 December 2016.

33 CJEU, joined cases C-511/18, C-512/18 and C-520/18, 6 October 2020.

34 CJEU, case C-623/17, 6 October 2020.

35 CJEU, case C-746/18, 2 March 2021.

3.1.1. Zadržavanje podataka

Sud pravde EU se na *svrhu zadržavanja* podataka naročito osvrnuo u odluci u predmetu *SpaceNet AG*. Pre svega, kada je reč o *opravdanosti ograničenja prava*, Sud je zauzeo stav da su ciljevi u prvoj rečenici čl. 15 st. 1 Direktive 2002/58/*EC*[36] navedeni taksativno, sledom čega zakonska mera doneta na osnovu te odredbe treba delotvorno i strogo da odgovara jednom od tih ciljeva, a da *postojanje mogućih poteškoća* da se *precizno utvrde slučajevi i uslovi* u kojima treba sprovesti ciljano zadržavanje *ne može da bude opravdanje* za državu članicu da propiše *opšte i neselektivno zadržavanje* podataka o saobraćaju i lokaciji komunikacija, *na način da izuzetak postane pravilo*.[37] Naime, Sud pravde EU je zauzeo jasan stav da nacionalno zakonodavstvo koje predviđa zadržavanje podataka treba da ispunjava *objektivne kriterijume*, uspostavljajući *vezu između podataka* koji treba da se zadrže *i cilja* koji se nastoji postići. Sud je našao da iz njegove sudske prakse proizlazi da, u skladu s načelom proporcionalnosti, postoji hijerarhija između tih ciljeva s obzirom na njihovu važnost i da upravo *važnost cilja*, koji se takvom merom nastoji ostvariti, *mora biti povezana s težinom zadiranja* u garantovana prava, koje iz toga proizlazi. Shodno tome, istakao je da je *pravu EU suprotno* nacionalno zakonodavstvo koje *u svrhu borbe protiv teških krivičnih dela kao pravilo predviđa opšte i neselektivno zadržavanje podataka* o saobraćaju i lokaciji komunikacije jer prekoračuje ono što je strogo nužno pa se ne može smatrati opravdanim u demokratskom društvu. Ističe se da se krivična dela, čak ni naročito teška, ne mogu izjednačiti s pretnjom po nacionalnu bezbednost. Naime, takvim izjednačavanjem bi se mogla stvoriti međukategorija – između nacionalne i javne bezbednosti – kako bi se na drugu kategoriju mogli primeniti zahtevi koji su svojstveni prvoj[38], što nije i ne može biti opravdano.

---

[36] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201/37 of 12/07/2002; Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, OJ L 337/11, of 18/12/2009.

[37] *SpaceNet AG*, para. 104–113.

[38] *SpaceNet AG*, para. 70–74, 92–94, 117–124.

Sud pravde EU je državama dao *jasne smernice* kako da u nacionalnim propisima *urede zadržavanje podataka na način koji nije protivan pravu EU*. Tako je u odluci u predmetu *Tele2 Sverige* državama članicama ostavljena mogućnost da nacionalnim zakonima predvide *ciljano zadržavanje* podataka o saobraćaju i lokaciji komunikacije u svrhu borbe protiv kriminala, ali uz postojanje *odgovarajućeg odobrenja i efektivnog nadzora* prilikom sprovođenja tih mera koje bi vršio sud ili nezavisno telo i uz poštovanje principa *vremenskog ograničenja* i u odnosu na ono *što je nužno i neophodno* za *konkretno određenu i opravdanu svrhu*.[39] Štaviše, u odluci u predmetu *La Quadrature du Net* Sud pravde EU je dao *smernice za pojedine oblike zadržavanja podataka* i zauzeo stav da se pravu EU ne protive određene mere, ukoliko su zakonom propisana jasna i precizna pravila, posebno ako su ispunjeni određeni *materijalni i formalni uslovi*, a naročito da pogođena lica imaju na raspolaganju *delotvorne garancije* protiv rizika i opasnosti od zloupotrebe.[40]

---

[39] *Tele2 Sverige*, para. 108–112, 116–125. Takođe, u toj odluci Sud pravde EU je izneo i stav da kada je reč o ciljevima koji mogu opravdati nacionalni propis kojim se odstupa od načela poverljivosti elektronskih komunikacija, treba podsetiti da, u meri u kojoj je, kako je to utvrđeno u para. 90 i 102 te presude, nabrajanje ciljeva u prvoj rečenici člana 15 stav 1 Direktive 2002/58 iscrpnog karaktera, pristup zadržanim podacima mora učinkovito i strogo ispunjavati jedan od tih ciljeva. Budući da cilj tog propisa mora biti u vezi s ozbiljnošću mešanja u temeljna prava koje uzrokuje taj pristup, iz toga sledi da u području sprečavanja, istrage, otkrivanja i progona krivičnih dela samo borba protiv teških krivičnih dela može opravdati takav pristup zadržanim podacima (vid. *Tele2 Sverige*, para. 115).

[40] Reč je o merama koje omogućavaju: a) *opšte i neselektivno zadržavanje podataka* o saobraćaju i lokaciji komunikacije *radi zaštite nacionalne bezbednosti* u situacijama u kojima je dotična država članica suočena s ozbiljnom pretnjom po nacionalnu bezbednost koja se pokazala stvarnom i trenutnom (neposrednom) ili predvidljivom, ako odluka kojom je predviđeno zadržavanje podataka može biti predmet delotvornog nadzora koji vrši sud ili nezavisan upravni organ, čija odluka ima obavezujući karakter, a kojom se nastoji proveriti da li postoji jedna od tih situacija i da li se poštuju uslovi i garancije koji se moraju predvideti, te ako se navedena odluka može izdati samo za razdoblje koje je vremenski ograničeno na ono što je strogo nužno, ali se može produžiti u slučaju nastavka postojanosti te opasnosti, b) *ciljano zadržavanje podataka* o saobraćaju i lokaciji *radi zaštite nacionalne bezbednosti, borbe protiv teških krivičnih dela i sprečavanja ozbiljnih pretnji javnoj bezbednosti*, koje je ograničeno na osnovu objektivnih i nediskriminatornih kriterijuma, zavisno od kategorije dotičnih lica ili posredstvom geolokacijskog kriterijuma, te koje se određuje za razdoblje čije je trajanje vremenski ograničeno na ono što je strogo nužno, ali se može produžiti; v) *opšte i neselektivno zadržavanje IP adresa* dodeljenih izvoru veze za razdoblje čije je trajanje vremenski ograničeno na ono što je strogo nužno, a *u svrhu zaštite nacionalne bezbednosti, borbe protiv teških krivičnih dela i sprečavanja ozbiljnih pretnji javnoj bezbednosti*; g) *opšte i neselektivno zadržavanje podataka* o građanskom identitetu korisnika elektronskih komunikacionih sredstava *u svrhu zaštite nacionalne bezbednosti, borbe protiv*

3.1.2. Pristup zadržanim podacima

U odluci u predmetu *Privacy International* Sud pravde EU je zaključio da je *pravu EU protivan* nacionalni propis, koji državnom organu omogućava da radi *zaštite nacionalne bezbednosti* naloži pružaocima elektronskih komunikacionih usluga *opšti i neselektivni prenos* podataka o saobraćaju i lokaciji komunikacije jer se time *prekoračuju granice onog što je strogo nužno* i ne može se smatrati opravdanim u demokratskom društvu. Čak i u slučaju konkretne ugroženosti nacionalne bezbednosti napominje se da se *propis ne sme ograničiti samo na to* da predvidi da zahtev za pristup zadržanim podacima odgovara ostvarenju propisanog cilja nego se moraju predvideti *materijalni i formalni uslovi* kojima se uređuje pristup podacima na osnovu objektivnih kriterijuma, kako bi se *definisale okolnosti i uslovi* pod kojima nadležnim organima može biti odobren pristup. Posebno treba voditi računa o tome da li je uspostavljen odnos između podataka čiji je prenos predviđen i pretnje po nacionalnu bezbednost te o tome da li postoji jasna veza između lica čijim zadržanim podacima će biti pristupljeno i konkretno određenog ugrožavanja nacionalne bezbednosti.[41] Takav zahtev *tim pre važi i za omogućavanje pristupa zadržanim podacima za potrebe krivičnog postupka*.

Sud pravde EU je u odluci u predmetu *Prokuratuur* zauzeo stav da *samo ciljevi borbe protiv teških krivičnih dela* ili sprečavanja ozbiljnih pretnji po javnu bezbednost mogu opravdati pristup državnih organa skupu podataka o saobraćaju ili lokaciji komunikacije, koji mogu pružiti

---

kriminala i zaštite javne bezbednosti; d) *hitno zadržavanje podataka* o saobraćaju i lokaciji komunikacija u određenom ograničenom trajanju kojima ti pružaoci usluga raspolažu *radi borbe protiv teških krivičnih dela i zaštite nacionalne bezbednosti*, na osnovu odluke nadležnog organa koja podleže delotvornom sudskom nadzoru, poštujući granice onoga što je strogo nužno; đ) *automatsku analizu i prikupljanje u stvarnom vremenu podataka* o saobraćaju i lokaciji komunikacije u slučaju da je ograničeno na situacije u kojima je država suočena s *ozbiljnom pretnjom po nacionalnu bezbednost* koja se pokazala stvarnom i trenutnom (neposrednom) ili predvidljivom, ako korišćenje takve analize može biti predmet delotvornog nadzora koji obavlja sud ili nezavisan upravni organ čija odluka ima obavezujući karakter, a kojom se nastoji proveriti da li postoji situacija koja opravdava navedenu meru i da li se poštuju uslovi i garancije koji se moraju predvideti i e) *prikupljanje u stvarnom vremenu tehničkih podataka* o lokaciji upotrebljene terminalne opreme, ukoliko je ograničeno na lica u odnosu na koja postoji opravdan i jasan razlog za sumnju da su na bilo koji način uključene *u terorističke aktivnosti*, i podleže prethodnom nadzoru koji obavlja sud ili nezavisni upravni organ, čija odluka ima obavezujući karakter, kako bi se osiguralo da se takvo prikupljanje u stvarnom vremenu odobri samo u granicama onoga što je strogo nužno. *La Quadrature du Net*, para. 168, 192. Više o tome Bugarski, Pisarić 2020.

41 *Privacy International*, para. 74–82.

informacije o komunikacijama koje je korisnik izvršio sredstvom elektronske komunikacije ili o lokaciji terminalne opreme kojom se koristi, a na osnovu kojih je moguće izvesti precizne zaključke o privatnom životu dotičnih lica, dok drugi činioci *ne mogu opravdati* takav pristup sa ciljem sprečavanja, istrage i otkrivanja *krivičnih dela uopšte*.[42] Dalje, pristup u načelu može biti odobren, s obzirom na cilj borbe protiv teškog kriminaliteta, *samo u odnosu na podatke lica* za koja postoji *jasna sumnja* da nameravaju da izvrše, da vrše ili su izvršili teško krivično delo ili da su na drugi način učestvovali u tom delu.[43] U svrhu osiguranja punog poštovanja tih uslova u praksi, bitno je da se *pre pristupa* nadležnih nacionalnih organa zadržanim podacima *sprovede nadzor* suda ili nezavisnog organa, povodom obrazloženog zahteva u okviru krivičnog postupka. Zahtev nezavisnosti, koji mora ispuniti organ zadužen za obavljanje prethodnog nadzora, nalaže da taj organ ima svojstvo treće strane u odnosu na organ koji zahteva pristup podacima, tako da može izvršiti nadzor objektivno i nepristrano i bez spoljašnjeg uticaja. Konkretno, zahtev nezavisnosti u krivičnom postupku podrazumeva da telo zaduženo za taj prethodni nadzor, s jedne strane, nije uključeno u sprovođenje predmetne krivične istrage i da, s druge strane, ima neutralan položaj u odnosu na stranke krivičnog postupka, odnosno da je takvog statusa da može osigurati pravednu ravnotežu između, s jedne strane, interesa povezanih s potrebama istrage u okviru borbe protiv kriminaliteta i, s druge strane, osnovnih prava na poštovanje privatnog života i zaštite podataka o ličnosti lica čiji su podaci obuhvaćeni pristupom. Zaključujući svoj stav, Sud pravde EU navodi da te kriterijume ne može ispunjavati javno tužilaštvo kao državni organ nadležan da vodi istragu i, zavisno od slučaja, zastupa optužbu, iz čega proizlazi da javno tužilaštvo nije u položaju da izvršava prethodni nadzor nad primenom

[42] U tom pogledu, Sud pravde EU je naveo da *čak i pristup ograničenoj količini podataka* ili pristup podacima *iz kratkog vremenskog razdoblja* može pružiti precizne informacije o privatnom životu korisnika sredstva elektronske komunikacije jer količina dostupnih podataka i konkretne informacije o privatnom životu dotičnog lica, koje iz njih proizlaze, predstavljaju okolnosti koje se mogu oceniti tek nakon pristupa tim podacima. Međutim, odobrenje suda ili nadležnog nezavisnog organa nužno se daje pre nego što se može pristupiti podacima i informacijama koje iz njih proizlaze, zbog čega se ocena ozbiljnosti zadiranja ostvarivanjem pristupa nužno vrši s obzirom na rizik koji je opštesvojstven kategoriji traženih podataka za privatni život dotičnih lica, pri čemu nije važno da se zna da li su informacije o privatnom životu koje iz njih proizlaze u konkretnom slučaju osetljive. *Prokuratuur*, para. 35–45.

[43] Ipak, u *posebnim okolnostima*, poput onih u kojima terorističke aktivnosti predstavljaju pretnju po ključne interese nacionalne bezbednosti, odbrane ili javne bezbednosti, pristup podacima *drugih lica* može se odobriti kad postoje objektivni elementi koji omogućavaju da se zaključi da ti podaci u konkretnom slučaju mogu dati stvaran i nedvosmislen doprinos borbi protiv takvih aktivnosti. *Prokuratuur*, para. 49–58.

mera pristupa zadržanim podacima.[44] Iz razloga opravdane hitnosti, moguće je sprovesti i naknadni nadzor, koji treba da usledi u kratkom vremenskom periodu po ostvarivanju pristupa podacima.[45]

3.2. Praksa ESLJP

Radi ispitivanja usklađenosti domaćeg pravnog okvira sa EKLJP, analizirane su odluke ESLJP u predmetima *Ekimdzhiev and others v. Bulgaria*,[46] *Škoberne v. Slovenia*[47] i *Podchasov v. Russia*,[48] povodom predstavki u kojima su podnosioci isticali da im je povređeno pravo iz čl. 8 EKLJP time što su pružaoci usluga zadržali njihove komunikacione podatke i što su nadležni organ pristupili tim podacima.

3.2.1. Ekimdzhiev and others v. Bulgaria

ESLJP je utvrdio da su, prema bugarskom zakonu, svi pružaoci komunikacionih usluga dužni da *zadrže* i šest meseci od okončanja komunikacije *čuvaju sve* podatke o pretplatniku, saobraćaju i lokaciji svih korisnika, s ciljem da ti podaci budu dostupni različitim nadležnim organima za određene, različite svrhe. Kako se od pružalaca zahteva da zadrže podatke koji se mogu, pojedinačno ili u kombinaciji s drugima, odnositi na „privatni život", takvo, zakonom propisano zadržavanje, samo po sebi, predstavlja mešanje u pravo na poštovanje privatnog života i prepiske, *bez obzira na to da li nadležni organi naknadno pristupaju zadržanim podacima*.[49] Pri tome, takvo mešanje se *može pripisati bugarskoj državi*, iako ga vrše privatna

[44] *Prokuratuur*, para. 51–59. Više o primeni principa proporcionalnosti i nezavisnosti organa u pogledu pristupa zadržanim podacima vid. Rovelli, Sophia. 2021. Case Prokuratuur: proportionality and the independence of authorities in data retention, *European Papers-A Journal on Law and Integration* 2021.1, 199–210.

[45] U pogledu pitanja da li se može nepostojanje prethodnog nadzora nezavisnog organa nadomestiti naknadnim sudskim nadzorom zakonitosti pristupa zadržanim podacima, Sud pravde EU je istakao da naknadni nadzor ne omogućava ispunjenje cilja prethodnog nadzora, koji se sastoji u sprečavanju da se odobri pristup predmetnim podacima koji prekoračuje granice onog što je strogo nužno. *Prokuratuur*, para. 49–58.

[46] ECtHR, *Ekimdzhiev and others v. Bulgaria* (Application no. 70078/12), January 11, 2022.

[47] ECtHR, *Škoberne v. Slovenia* (Application no. 19920/20), 15 February 2024.

[48] ECtHR, *Podchasov v. Russia* (Application no. 33696/19), 13 February 2024.

[49] *Ekimdzhiev and others v. Bulgaria*, para. 372.

lica, jer su na to obavezana zakonom.[50] ESLJP je dalje našao da bugarski nadležni organi mogu da *pristupe* zadržanim komunikacionim podacima, ako je to neophodno radi ostvarivanja jednog ili više zakonom određenih ciljeva. Prema mišljenju ESLJP, kako komunikacioni podaci bilo kog lica teoretski mogu postati neophodni za jednu ili više tih svrha, to i podnosioci predstavke mogu biti pogođeni osporenim zakonodavstvom. Zbog toga je ESLJP utvrdio da *pristup nadležnih organa* zadržanim komunikacionim podacima predstavlja *dalje mešanje* u pravo iz čl. 8 EKLJP. [51] Povodom *opravdanosti* mešanja u pravo iz čl. 8 EKLJP, ESLJP je istakao da zadržavanje komunikacionih podataka od pružalaca usluga i naknadni pristup od državnih organa u pojedinačnim slučajevima moraju biti praćeni, *mutatis mutandis*, *istim merama zaštite kao i tajni nadzor komunikacije*.[52]

Iako bugarsko zakonodavstvo propisuje određene mere zaštite s ciljem da nadležni organi pristupaju zadržanim komunikacionim podacima samo kada je to opravdano, s obzirom na to da je potrebno prethodno *odobrenje suda*, prema oceni ESLJP, to je ipak *ispod zahtevanog standarda delotvornosti zaštite*.[53] Kada je reč o *„sudbini" zadržanih podataka* kojima pristupaju

[50] *Ekimdzhiev and others v. Bulgaria*, para. 375. Identičan stav ESLJP je zauzeo u predmetu *Podchasov v. Russia* koji se odnosio na zakonsku obavezu pružaoca internet komunikacionih usluga da sve podatke o komunikaciji čuva godinu dana, a sadržaj svih komunikacija šest meseci i da omogući pristup tim podacima i dostavi ih organima za sprovođenje zakona ili službama bezbednosti u okolnostima određenim zakonom, zajedno sa informacijama neophodnim za dešifrovanje elektronskih poruka ako su šifrovane (para. 50–52), kao i u predmetu *Škoberne v. Slovenia* koji se odnosio na obavezu pružalaca telekomunikacionih usluga da podatke o saobraćaju i lokaciji koji se odnose na fiksnu i mobilnu telefoniju svih korisnika telekomunikacionih usluga zadrže i čuvaju 14 meseci i po zahtevu dostave nadležnim organima za određene svrhe sprovođenja zakona, pri čemu različiti organi mogu pristupiti tim podacima (para. 125–128).

[51] *Ekimdzhiev and others v. Bulgaria*, para. 376.

[52] Sud je istakao da, s obzirom na tehnološki i društveni razvoj u poslednje dve decenije u oblasti elektronskih komunikacija, komunikacioni podaci mogu otkriti veliki broj podataka o ličnosti, te ukoliko ih nadležni organi pribavljaju masovno, mogu se koristiti za stvaranje intimne slike o licu, kroz mapiranje društvenih mreža, praćenje lokacije, praćenje pretraživanja interneta, mapiranje obrazaca komunikacije i uvid u to sa kim je to lice komuniciralo i kada i sl. Pribavljanje tih podataka *putem masovnog i opšteg zadržavanja i pristupa* zadržanim podacima stoga može biti *jednako nametljivo kao i masovno prikupljanje sadržaja komunikacija*, zbog čega njihovo presretanje, zadržavanje i korišćenje od nadležnih organa treba analizirati *u kontekstu mera zaštita* koje se odnose na sadržaj komunikacije. *Ekimdzhiev and others v. Bulgaria*, para. 394–395.

[53] Sud je utvrdio da se u zahtevima za pristup koji se podnose van okvira već pokrenutih krivičnih postupaka navode osnov i svrha traženja pristupa zadržanim podacima, kao i potpuni prikaz okolnosti koje pokazuju da su podaci potrebni za

nadležni organi, ESLJP je došao do zaključka da se ti podaci jednostavno čuvaju u spisima krivičnog predmeta, da prate njegovu sudbinu i da im može pristupiti svako ko ima pristup samom spisu, pa se *ne može prihvatiti da postoji odgovarajući nivo zaštite podataka* jer *ne postoje odredbe koje na adekvatan način uređuju* čuvanje, pristup, ispitivanje, korišćenje, saopštavanje i uništavanje podataka.[54] U pogledu *obaveštavanja lica* čijim zadržanim podacima se pristupilo, ESLJP je našao da propisano obaveštavanje *nije u skladu sa utvrđenom sudskom praksom*[55] jer je obaveštenje *potrebno u svim slučajevima*, a ne samo u onim u kojima se podacima pristupilo nezakonito, i to čim se može izvršiti bez ugrožavanja svrhe preduzete mere.[56] Dalje,

tačno određenu i relevantnu svrhu. Nasuprot tome, u pogledu *zahteva za pristup u vezi sa krivičnim postupkom*, iako bi trebalo da sadrže informacije o navodnom krivičnom delu u vezi sa kojim se pristup traži, *nadležni organi nisu izričito obavezani* da u zahtevu objasne zašto su ti podaci zaista potrebni (samo treba da sadrži opis okolnosti koje su u osnovi zahteva) niti da sudiji „u potpunosti i iskreno" otkriju sva pitanja koja su relevantna za ocenu osnovanosti zahteva za pristup, uključujući pitanja koja mogu „oslabiti" opravdanost zahteva, pa ni da prilože prateći materijal – što sudiju može onemogućiti da pravilno proceni da li je zahtev za pristup osnovan. Takođe, *zakon ne obavezuje sudiju*, koji ispituje zahteve za pristup, da u odluci kojom odobrava pristup navede *razloge* koji objašnjavaju zašto je odlučio da je odobravanje zaista bilo neophodno i srazmerno, odnosno da se manje invazivnim merama nije mogla postići ista svrha. *Ekimdzhiev and others v. Bulgaria*, para. 400–407.

[54] Relevantno zakonodavstvo Bugarske predviđa da svi komunikacioni podaci *koji nisu korišćeni za pokretanje krivičnog postupka* moraju biti uništeni u roku od tri meseca od dana prijema od nadležnih organa, a da svi podaci kojima se pristupilo po hitnom postupku moraju biti odmah uništeni na isti način, ukoliko takav pristup nije retrospektivno potvrđen od nadležnog sudije. Nasuprot tome, *takav rok nije određen* za podatke kojima je pristupljeno *a pokrenut je krivični postupak*. ESLJP je istakao da, iako se čini da je to pitanje pokriveno internim pravilima koje je izdao glavni tužilac, ta pravila nisu učinjena dostupnim javnosti, pa je nejasno šta predviđaju. Takođe, ništa ne sugeriše da su odredbe odgovarajućeg zakona radi transponovanja Direktive (EU) 2016/680 do sada korišćene za popunjavanje te praznine. *Ekimdzhiev and others v. Bulgaria*, para. 408–409.

[55] Iako bugarski Zakon o elektronskim komunikacijama zahteva od specijalnog parlamentarnog odbora da *obavesti* pojedinca u slučaju da se njegovim zadržanim komunikacionim podacima *nezakonito* pristupilo ili je nezakonito traženo da im se pristupi, pod uslovom da takvo obaveštenje ne bi ugrozilo svrhu zbog koje se tim podacima pristupa, ESLJP je našao da takvo rešenje nije zadovoljavajuće.

[56] Sud je našao da ništa ne ukazuje na to da je takvo obaveštenje do sada učinjeno na osnovu izmena i dopuna zakona radi transponovanja Direktive (EU) 2016/680 gde je amandmanima predviđena mogućnost pojedincima da dobiju takve informacije o zadržanim i pristupljenim komunikacionim podacima, niti se čini da je do sada bilo slučajeva u kojima su lica mogla da dobiju informacije o zadržavanju ili pristupu svojim komunikacionim podacima u skladu sa relevantnim odredbama

ESLJP je utvrdio da ni Zakon o elektronskim komunikacijama ni Zakon o krivičnom postupku ne predviđaju *pravni lek* u vezi sa zadržavanjem ili pristupom komunikacionim podacima.[57] Konačno, u pogledu nadzora nad ostvarivanjem pristupa zadržanim podacima, ESLJP je zaključio da postojeći mehanizmi nisu podobni da osiguraju da se ovlašćenja za pristup podacima ne zloupotrebljavaju.[58]

---

tog zakona. U nedostatku daljih detalja, ne može se prihvatiti da su odredbe o zaštiti podataka u vezi sa zadržanim komunikacionim podacima efektivne u tom pogledu. *Ekimdzhiev and others v. Bulgaria*, para. 416–417.

[57] Takođe, ukazano je na to da se, usled nedostatka detalja o „stvarnom funkcionisanju" sistema pravnih lekova u vezi sa komunikacionim podacima, ne može prihvatiti da su novouvedena pravna sredstva, u nedostatku prijavljenih odluka bugarskih sudova, trenutno zaista i delotvorna i da ne postoji bilo kakav dokaz da je pravni lek dostupan. Iz toga sledi da se zabrinutost javnosti u vezi sa pretnjom zloupotrebe pristupa i korišćenja komunikacionih podataka od državnih organa ne može u dovoljnoj meri otkloniti postojanjem delotvornih pravnih lekova u tom pogledu. Naime, na državi je da objasni da je obezbeđena delotvornost pravnih lekova, za koje tvrdi da su efikasna, i da pružena objašnjenja, koliko god je to moguće, potkrepi konkretnim primerima, što je u slučaju Bugarske izostalo. *Ekimdzhiev and others v. Bulgaria*, para. 376–382.

[58] Naime, Komisija za zaštitu podataka o ličnosti nadležna je da nadzire postupanje pružalaca komunikacionih usluga, ali *nema izričita ovlašćenja u odnosu na državne organe* koji mogu pristupiti zadržanim podacima. Osim toga, iako su, relevantnim izmenama i dopunama zakonodavstva radi transponovanja Direktive (EU) 2016/680, ova Komisija i Inspektorat pri Vrhovnom veću sudstva zaduženi da nadgledaju način na koji državni organi obrađuju podatke o ličnosti u svrhe sprovođenja zakona, ništa ne sugeriše da su ova tela do sada koristila ta ovlašćenja u vezi sa zadržanim komunikacionim podacima. Takođe, sudija koji odobrava pristup zadržanim podacima nije u poziciji da obezbedi efikasnu kontrolu jer, iako mu nadležni organi dostavljaju izveštaj o sprovedenoj meri, *nema ovlašćenja* da vrši nadzor ni da naloži korektivne mere, nije ovlašćen niti se od njega očekuje da vrši inspekciju na licu mesta, a svoje nadzorne dužnosti obavlja isključivo na osnovu izveštaja nadležnih organa. Osim toga, iako glavno nadzorno telo – *specijalni parlamentarni odbor* – može da nadzire i pružaoce komunikacionih usluga i nadležne organe i ima široka ovlašćenja za prikupljanje informacija i nadzor, a godišnji izveštaji pokazuju da redovno sprovodi inspekcije preko službenika koje zapošljava, nedostatak se ogleda u tome što njegovi članovi ne moraju biti lica sa pravnim kvalifikacijama ili iskustvom u toj oblasti, a odbor nema ovlašćenja da naloži korektivne mere u konkretnim slučajevima već može samo da izda uputstva osmišljena da poboljšaju relevantne procedure te ako otkrije nepravilnosti, može samo da skrene pažnju nadležnim organima ili obavesti rukovodioce relevantnih organa i pružaoce komunikacionih usluga. *Ekimdzhiev and others v. Bulgaria*, para. 410–415.

3.2.2. Škoberne v. Slovenia

ESLJP je utvrdio da je (izmenjeni) Zakon o elektronskim komunikacijama iz 2004. godine *odredio brojne svrhe* u koje je trebalo da se čuvaju komunikacioni podaci, *ali nije sadržao* odredbe koje bi *ograničile obim i primenu mere* samo na ono što je bilo neophodno za postizanje tih svrha, pri čemu država nije pokazala da je drugi zakonski akt sadržao takve odredbe. ESLJP je najpre ukazao na to da iz postojeće sudske prakse proizilazi da nacionalni zakon treba, kao deo minimalnih zahteva, na način koji odgovara određenoj meri nadzora, da definiše obim primene mere nadzora i obezbedi odgovarajuće procedure za odobravanje i/ili preispitivanje s ciljem da mera ostane u granicama neophodnog. Naime, trebalo je da minimalni zahtevi budu ispunjeni i u pogledu zadržavanja komunikacionih podataka, imajući u vidu prirodu spornog mešanja. S tim u vezi, ESLJP je istakao da se nedvosmislenost zakona, koji *kao pravilo propisuje opšte i neselektivno zadržavanje* komunikacionih podataka, ne može smatrati dovoljnom garancijom njegove usklađenosti sa principima vladavine prava i proporcionalnosti. Nepostojanje odredaba ili mehanizama koji bi osigurali da mera bude zapravo ograničena na ono što je „neophodno u demokratskom društvu" za specifične svrhe navedene u (izmenjenom) Zakonu iz 2004. godine, te određivanje čuvanja zadržanih podataka na period od 14 meseci, učinilo je takav *režim nepomirljivim sa obavezama države* prema čl. 8 EKLJP.[59]

Potkrepljujući svoje navode, ESLJP se poziva i na praksu Suda pravde EU i napominje da *režim obaveznog opšteg i neselektivnog zadržavanja* komunikacionih podataka u svrhu borbe protiv teškog kriminala nije u skladu sa zahtevom proporcionalnosti, te da čak i u kontekstu zaštite nacionalne bezbednosti, gde bi se zadržavanje komunikacionih podataka moglo naložiti kao opšta i neselektivna mera pod određenim strogim uslovima, takvo zadržavanje ne može biti sistemske prirode nego mora biti predmet nezavisnog nadzora u konkretnom slučaju.[60]

Razmatrajući mogućnost upotrebe podataka prikupljenih u takvom režimu zadržavanja, ESLJP je istakao da je, bez obzira na to što su Sud pravde EU i Ustavni sud Slovenije režim zadržavanja proglasili nevažećim, za ocenu da li je u konkretnom slučaju postupanje bilo u skladu sa čl. 8 EKLJP relevantan trenutak kada su ti podaci zadržani i kada im se pristupilo (a to je bilo pre nego što je dotični režim proglašen nevažećim) i da li je

[59] *Škoberne v. Slovenia*, para. 138–139.

[60] *Škoberne v. Slovenia*, para. 140, 68.

podnosilac predstavke, u vreme kada su zadržani komunikacioni podaci, uživao adekvatnu pravnu zaštitu, na koju je imao pravo prema Konvenciji – a Sud smatra da to nije bio slučaj. Dalje, ESLJP je naglasio da, iako je pristup podacima podnosioca predstavke bio praćen određenim zaštitnim merama (tj. sudskim odobrenjem), zaštitne mere, same po sebi, nisu bile dovoljne da učine režim zadržavanja usklađenim sa čl. 8 EKLJP.[61]

Zaključujući, ESLJP je izneo stanovište da je, bez obzira na količinu podataka, u smislu čl. 8 EKLJP, važno da su podaci zadržani u okviru opšteg i neselektivnog režima, za koji je utvrdio da je u suprotnosti sa čl. 8 EKLJP.[62] Drugim rečima, kada se utvrdi da zadržavanje komunikacionih podataka predstavlja *kršenje čl. 8 EKLJP* jer nije ispoštovan zahtev „kvaliteta zakona" i/ili princip proporcionalnosti, *isto važi i za pristup zadržanim podacima* i njihovu naknadnu obradu od državnih organa.[63]

3.2.3. Podchasov v. Russia

U odluci u tom predmetu ESLJP je, između ostalog, našao da *samo postojanje zakona* koje zahteva *kontinuirano i automatsko zadržavanje i čuvanje* od pružalaca elektronskih komunikacija svih podataka o internet komunikaciji i srodnih komunikacionih podataka, kao i čuvanje sadržaja svih internet

---

[61] *Škoberne v. Slovenia*, para. 142–143. Štaviše, ESLJP je primetio da je Sud pravde EU na sličan način, u predmetima *SpaceNet* i *Telekom Deutschland*, našao da *nacionalno zakonodavstvo*, koje je obezbedilo puno poštovanje uslova utvrđenih putem zakona kojim se implementira Direktiva 2006/24/*EC*, u vezi sa pristupom zadržanim podacima, *ne može*, po svojoj prirodi, *da ograniči ili čak ispravi ozbiljne smetnje koje proizilaze iz opšteg zadržavanja podataka*, pri čemu su zadržavanje i pristup takvim podacima odvojena mešanja u pravo koja *zahtevaju posebna opravdanja*. *Škoberne v. Slovenia*, para. 87.

[62] Sud je naveo da *nije* od nekog posebnog *značaja* to što su, osuđujući podnosioca predstavke, domaći sudovi koristili *ograničenu količinu* zadržanih podataka koji su se odnosili na (*ograničen*) *period* od mesec dana jer se predstavka odnosi na čitav niz podataka koji su zadržani i čuvani u periodu od četrnaest meseci, a koje su pribavili nadležni organi, a zatim obradili, čuvali i ispitali za potrebe predmetnog krivičnog postupka. *Škoberne v. Slovenia*, para. 145, 147.

[63] *Škoberne v. Slovenia*, para. 144. U vezi sa tim, ESLJP se pozvao na stav koji je izrazio Sud pravde EU u predmetu *An Garda Siochana*, gde je Sud pravde EU utvrdio da komunikacijski podaci ne mogu biti predmet opšteg i neselektivnog zadržavanja u svrhu borbe protiv teškog kriminala i da stoga pristup takvim podacima ne može biti opravdan u tu istu svrhu, te saglasno tome ESLJP ne vidi razlog da utvrdi drugačije u vezi sa slučajem podnosioca predstavke.

komunikacionih usluga koje se koriste za prenos glasovnih, tekstualnih, vizuelnih, zvučnih, video ili drugih elektronskih komunikacija, *potencijalni pristup nadležnih organa* tim podacima i obaveza Telegrama da ih dešifruje, ukoliko su šifrovani, predstavlja izuzetno *ozbiljno i neprihvatljivo mešanje* u prava podnosioca predstavke iz čl. 8 EKLJP. Sud je istakao da se na taj način faktički utiče na sve korisnike internet komunikacija, naročito u situaciji kada ne postoji određeni stepen sumnje da su umešani u kriminalne aktivnosti ili aktivnosti koje ugrožavaju nacionalnu bezbednost, odnosno kada ne postoji drugi razlog da se veruje da zadržavanje podataka može doprineti borbi protiv teškog kriminala ili zaštiti nacionalne bezbednosti.[64] Tako široko propisana obaveza zadržavanja podataka, *bez ikakvog ograničenja obima mere* u smislu teritorijalne ili vremenske primene ili kategorija lica čiji se lični podaci zadržavaju i čuvaju, ozbiljno ugrožava prava iz čl. 8 EKLJP.[65]

Osim toga, ESLJP, kao posebno invazivnu, ističe *obavezu pružalaca usluga* elektronskih komunikacija *da instaliraju opremu* koja nadležnim organima omogućava *direktan, daljinski pristup* svim zadržanim podacima o internet komunikacijama, kao i sadržaju ostvarene komunikacije, čime im se omogućava da zaobiđu proceduru autorizacije i pristupe sačuvanim zadržanim komunikacionim podacima i sadržaju ostvarene komunikacije bez prethodnog sudskog odobrenja. Takva praksa je, prema stavu ESLJP, neprihvatljiva, imajući u vidu da zahtev da se pružaocu komunikacionih usluga, pre ostvarivanja pristupa zadržanim podacima, dostavi prethodno sudsko odobrenje predstavlja važnu zaštitu od zloupotrebe od nadležnih organa, dok nepostojanje takvog prethodnog sudskog odobrenja u velikoj meri povećava stepen proizvoljnosti i mogućnosti (sklonosti) ka zloupotrebi, čime nisu ispunjeni minimalni zahtevi za zaštitnim merama.[66]

---

[64] Istaknuto je da bi zaštita predviđena čl. 8 EKLJP bila neprihvatljivo oslabljena kada bi se upotreba modernih tehnologija u sistemu krivičnog pravosuđa dozvolila po svaku cenu i bez pažljivog balansiranja između potencijalnih koristi od ekstenzivne upotrebe takvih tehnologija i važnih interesa zaštite privatnog života, odnosno zaštite podataka o ličnosti. *Podchasov v. Russia*, para. 62.

[65] *Podchasov v. Russia*, para. 70.

[66] *Podchasov v. Russia*, para.72–75. Važno je napomenuti i to da u istoj odluci, u pogledu zahteva da se bezbednosnim službama dostavljaju informacije koje su neophodne za dešifrovanje elektronskih komunikacija ako su šifrovane, ESLJP primećuje da šifrovanje pruža snažne tehničke garancije protiv nezakonitog pristupa sadržaju komunikacija i stoga se naširoko koristi kao sredstvo zaštite prava na poštovanje privatnog života i privatnosti prepiske na mreži. U digitalnom dobu, tehnička rešenja

4. USAGLAŠENOST DOMAĆEG PRAVNOG OKVIRA SA STANDARDIMA ZAŠTITE LJUDSKIH PRAVA

Pojedini stavovi koje su Sud pravde EU i ESLJP izneli u odlukama u pomenutim predmetima potencijalno su primenjivi i na domaći pravni okvir.

4.1. Usaglašenost sa pravom EU

ZEK iz 2010. usvojen je po uzoru na Direktivu 2006/24/ *EC*, a pojedini delovi su prosto prevedeni i integrisani u zakon, odnosno preuzeti su nekritički i bez potrebnog nomotehničkog prilagođavanja (imajući u vidu pravnu prirodu direktiva). U naknadnim zakonskim intervencijama nisu uzeti u obzir stavovi Suda pravde EU jasno izraženi u odluci kojom je poništena Direktiva 2006/24/*EC*[67] ni stavovi iz nekoliko odluka povodom nacionalnih propisa,[68] a to nije učinjeno ni prilikom donošenja novog zakona 2023. godine.

U pogledu *zadržavanja podataka*, argumenti zbog kojih je Direktiva 2006/24/*EC* stavljena *van snage* – jer se široko i osobito teško mešala u osnovna ljudska prava, a da pritom takvo mešanje nije bilo precizno ograničeno na ono što je strogo nužno – mogu se bez problema *primeniti i na srpski zakon*.[69] Sud pravde EU je odredio da je *nacionalni propis* kojim

za obezbeđivanje i zaštitu privatnosti elektronskih komunikacija, uključujući mere za šifrovanje, doprinose obezbeđivanju uživanja drugih osnovnih prava, kao što je sloboda izražavanja. Štaviše, čini se da šifrovanje pomaže građanima i preduzećima da se odbrane od zloupotreba informacionih tehnologija, kao što su hakovanje, krađa identiteta i ličnih podataka, prevara i neprikladno otkrivanje poverljivih informacija. Saglasno tome, imajući u vidu da bi bilo neophodno oslabiti šifrovanje za sve kako bi se omogućilo dešifrovanje komunikacija zaštićenih *end-to-end* enkripcijom, te da se na taj način mere ne mogu ograničiti na određene pojedince i da bi neselektivno uticale na sve, uključujući i pojedince koji nisu pretnja legitimnom interesu vlade, slabljenje enkripcije stvaranjem *backdoor*-a očigledno bi učinilo tehnički mogućim obavljanje rutinskog, opšteg i neselektivnog nadzora ličnih elektronskih komunikacija, te da kriminalne mreže takođe mogu da iskoriste *backdoor* i ozbiljno ugroze bezbednost elektronskih komunikacija svih korisnika, ESLJP uzima u obzir opasnosti ograničavanja šifrovanja koje su opisali mnogi stručnjaci u toj oblasti, pa shodno svemu tome zaključuje da zakonska obaveza pružaoca internet komunikacija da dešifruje *end-to-end* šifrovanu komunikaciju predstavlja rizik da provajderi takvih usluga oslabe mehanizam šifrovanja za sve korisnike i da se postojanje takve obaveze ne može smatrati srazmernim legitimnim ciljevima kojima se teži. *Podchasov v. Russia*, para. 76–79.

67 Više o tome Pisarić 2019, 187–188.

68 Više o tome Mitsilegas *et al*. 2023, 182–183.

69 Vid. posebno para. 25–29, 54–69.

je predviđeno *opšte i neselektivno zadržavanje* svih podataka o saobraćaju i lokaciji svih korisnika usluga elektronske komunikacije *nedozvoljen i prekomeran* u odluci iz 2016. u predmetu *Tele2 Sverige*. To je potvrdio, između ostalog, i u odlukama u predmetu *La Quadrature du Net* iz 2020. i u predmetu *SpaceNet AG* iz 2022. godine. Analogno tome, nije teško doći do odgovora na pitanje da li je ZEK, koji propisuje obavezu opšteg i neselektivnog zadržavanja podataka o elektronskim komunikacijama, *bez određivanja svrhe zbog koje se podaci zadržavaju*, u skladu sa pravom EU. Pri tome, treba imati u vidu da Sud pravde EU zauzeo jasan stav da *zadržavanje i pristup* zadržanim podacima predstavljaju *odvojena mešanja* u garantovana prava koja zahtevaju posebna opravdanja.

S tim u vezi, a u pogledu pristupa zadržanim podacima za potrebe krivičnog postupka, upitno je da li i u kojoj meri odredbe ZKP ispunjavaju zahteve utvrđene u praksi Suda pravde EU. Svrha ostvarivanja pristupa proizlazi iz čl. 286 st. 3 ZKP, u kojem stoji da je policija ovlašćena da pristupi zadržanim podacima „u cilju ispunjenja dužnosti iz stava 1. ovog člana".[70] Ne bi se moglo reći da je tom formulacijom dovoljno precizno određena svrha ostvarivanja pristupa u pojedinom slučaju jer nije dovoljno da se prosto propiše da policija može da pristupi zadržanim podacima radi ostvarivanja određenog cilja (odnosno dužnosti iz čl. 286 st. 1).[71] Naime, iako su odredbama ZKP propisani uslovi za pristup zadržanim podacima: materijalni („ako postoje osnovi sumnje da je izvršeno krivično delo za koje se goni po službenoj dužnosti") i formalni (da je javni tužilac podneo zahtev a sudija za prethodni postupak nalogom odobrio prikupljanje podataka), iz prakse Suda pravde EU nedvosmisleno proizlazi da *uslovi treba da se zasnivaju na objektivnim kriterijumima*, kojim bi se bliže odredile okolnosti pod kojima nadležnim organima može biti odobren pristup u pojedinom slučaju, što je u ZKP izostalo. Što se tiče materijalnog uslova da postoji najniži stepen sumnje da je izvršeno bilo koje krivično delo za koje se goni po službenoj dužnosti, treba imati u vidu da je Sud pravde EU zauzeo stav da režim *opšteg i neseleketivnog prenosa* zadržanih podataka nadležnim organima, pa i u svrhu borbe *protiv teškog kriminala*, nije u skladu sa zahtevom kvaliteta zakona i/ili proporcionalnosti – tim pre, to bi važilo za pristup zadržanim podacima u svrhu borbe protiv kriminala uopšte, kako je to predviđeno ZKP-om. Pri tome, mera iz čl. 286 st. 3 ZKP se može odrediti u odnosu

[70] Odnosno „da se pronađe učinilac krivičnog dela, da se učinilac ili saučesnik ne sakrije ili ne pobegne, da se otkriju i obezbede tragovi krivičnog dela i predmeti koji mogu poslužiti kao dokaz, kao i da prikupi sva obaveštenja koja bi mogla biti od koristi za uspešno vođenje krivičnog postupka".

[71] Vid. *Privacy International*, para. 74–81.

na bilo koje lice (dakle, čak i u odnosu na lice za koje ne postoji nikakva naznaka da njihovo ponašanje može imati vezu, čak i posrednu ili daleku, s ciljem vođenja krivičnog postupka), a Sud pravde EU je istakao da bi se pristup mogao odrediti samo u odnosu na podatke lica za koja postoji jasna sumnja da su izvršili teško krivično delo, dok bi u pogledu podataka drugih lica pristup mogao da bude odobren samo pod restriktivnim uslovima.[72] U pogledu formalnog uslova, iz prakse Suda pravde EU proizlazi da posebno treba voditi računa o tome da li je uspostavljen odnos između podataka čiji se prenos traži i krivičnog dela te da li postoji jasna veza između lica čijim zadržanim podacima će biti pristupljeno i konkretnog krivičnog postupka,[73] što bi trebalo da bude *obrazloženo* i u zahtevu nadležnog organa za pristup i u odluci suda kojim se odobrava pristup u konkretnom slučaju,[74] dok ZKP ne postavlja takav zahtev ni za predlog ni za nalog.

Osim toga, čini se da Srbija do sada nije razmotrila mogućnost da normira *ciljano zadržavanje* podataka i pristup tim podacima onako kako se sugeriše u odlukama Suda pravde EU, koje sadrže dosta jasne smernice i kriterijume za što izbalansiraniji pristup rešavanju odnosa zaštite javnog interesa i mešanja u osnovna ljudska prava (kao što je npr. određeno u predmetu *La Quadrature du Net*).

Zbog svega rečenog, a nakon analize relevantne prakse Suda pravde EU ne bi se moglo tvrditi da su nacionalni propisi u Srbiji usaglašeni sa pravom EU, a Srbija bi, kao kandidat za članstvo u EU, trebalo da uzme u obzir stavove i smernice utvrđene u odlukama najvišeg suda EU. Ozbiljnost (ne) adekvatnosti zakonskih rešenja sagledava se dodatno u (ne)usaglašenosti s praksom ESLJP.

4.2. Usaglašenost sa EKLJP

Polazeći od prikazane prakse ESLJP, moglo bi se reći da svi korisnici usluga elektronskih komunikacija u Srbiji imaju *status žrtve mešanja* u njihova prava iz čl. 8 EKLJP *zbog načina na koji propisi obavezuju* operatore da *zadrže i čuvaju* veliki broj podataka o elektronskim komunikacijama svih

[72] Vid. *Prokuratuur*, para. 49–58.

[73] Vid. *Privacy International*, para. 74–81.

[74] Više o tome u 4.2.1.

svojih korisnika (i to bez obzira na to da li im nadležni organi naknadno pristupaju) i na koji *uređuju pristup zadržanim podacima* od strane nadležnih organa za potrebe krivičnog postupka.[75]

Dalje, kako svrha zadržavanja podataka u ZEK nije određena, pa samim tim ne postoje ni odredbe koje bi ograničile obim i primenu zadržavanja na ono što je neophodno za postizanje svrhe, nego postoji opšti i neselektivni režim zadržavanja podataka, moglo bi se zaključiti da je takvo *zadržavanje u suprotnosti sa čl. 8 EKLJP* jer nije poštovan zahtev „kvaliteta zakona" i/ili princip proporcionalnosti. Isto važi i za *pristup zadržanim podacima* i njihovu naknadnu obradu od nadležnih državnih organa za potrebe krivičnog postupka, kako je to uređeno u ZKP.[76]

U pogledu *opravdanosti* takvog mešanja u pravo iz čl. 8 EKLJP, u nastavku ćemo analizirati odredbe ZEK, kao propisa kojim se uređuju zadržavanje i pristup zadržanim podacima u načelu, odredbe ZKP, kao propisa kojim se uređuje pristup zadržanim podacima za potrebe krivičnog postupka, i odredbe drugih propisa, u svetlu stava ESLJP da, s obzirom na značaj komunikacionih podataka, zadržavanje od pružalaca usluga i naknadni pristup državnih organa u pojedinačnim slučajevima moraju biti praćeni *istim merama zaštite kao i tajni nadzor komunikacije*.[77]

4.2.1. Zahtev/odluka

U pogledu *prethodnog odobravanja pristupa* zadržanim podacima, kao zaštitne mere koja bi trebalo da obezbedi da nadležni organi pristupaju zadržanim komunikacionim podacima samo kada je to opravdano, postavlja se pitanje da li je to pitanje u ZKP uređeno na adekvatan način. *Odredbama ZKP nije propisano* šta bi predlog javnog tužioca, kao zahtev nadležnog organa za odobrenje pristupa, odnosno nalog sudije za prethodni postupak, kao odluka kojom se pristup odobrava, trebalo da sadrže,[78] *ne zahteva se* da budu obrazloženi uopšte, a kamoli da se pokaže da je ispunjen uslov da se manje

[75] Vid. *Ekimdzhiev and others v. Bulgaria*, para. 372, 376; *Podchasov v. Russia*, para. 50–52; *Škoberne v. Slovenia*, para. 125–128.

[76] Vid. *Škoberne v. Slovenia*, para. 144.

[77] Vid. *Ekimdzhiev and others v. Bulgaria*, para. 394–395; *Podchasov v. Russia*, para. 72; *Škoberne v. Slovenia*, para. 119, 133–134, 137.

[78] Prema postojećem zakonskom rešenju, dovoljno bi bilo da zahtev sadrži navod da postoje osnovi sumnje da je izvršeno određeno krivično delo za koje se goni po službenoj dužnosti i da pristup zadržanim podacima treba ostvariti kako bi se pronašao učinilac krivičnog dela, da se učinilac ili saučesnik ne bi sakrio ili pobegao,

invazivnim merama nije mogla postići ista svrha. Iz toga sledi da procedura za ovlašćivanje nadležnih organa da pristupe zadržanim komunikacionim podacima ne garantuje efektivno da se takav pristup odobrava samo kada je to zaista neophodno i proporcionalno u konkretnom slučaju.[79] Zbog svega toga bi se moglo reći da čl. 286 st. 3 ZKP *ne ispunjava standard kvaliteta zakona* u pogledu ostvarivanja pristupa zadržanim podacima, kako je to uobličeno u praksi ESLJP.

Takođe, kako je ESLJP negativno reagovao na propisanu *obavezu pružalaca* elektronskih komunikacija *da instaliraju opremu* koja nadležnim organima *omogućava direktan*, *daljinski pristup zadržanim podacima*, trebalo bi se osvrnuti na domaće propise. Iako iz ZEK nedvosmisleno proizlazi da je postojanje sudske odluke neophodan prethodni uslov za oba načina pribavljanja zadržanih podataka (čl. 128 st. 7), treba pažljivo razmotriti obaveze operatora u vezi sa *tehničkim interfejsom*.[80] Osim toga, iako se podatak o sudskoj odluci, koja je osnov za pristup zadržanim podacima, unosi u evidencije koje vode operatori i nadležni organi koji ostvaruju pristup zadržanim podacima (čl. 128 st. 8 i st. 9 ZEK), njihova obaveza *da kao tajnu čuvaju te evidencije*, i to u skladu sa Zakonom o tajnosti podataka[81] (ZTP), ne doprinosi otklanjanju potencijalne sumnje da nadležni organi mogu *faktički da zaobiđu proceduru autorizacije* i pristupe zadržanim podacima direktno, bez prethodnog sudskog odobrenja.[82]

4.2.2. Obaveštavanje lica

U pogledu obaveštavanja lica na koje se odnose zadržani podaci kojima su nadležni organi pristupili, ESLJP je istakao da je obaveštenje *potrebno u svim slučajevima*, čim se obaveštavanje može izvršiti *bez ugrožavanja svrhe* zbog

---

kako bi se otkrili i obezbedili tragovi krivičnog dela i predmeti koji mogu poslužiti kao dokaz, odnosno da bi se prikupila sva obaveštenja koja bi mogla biti od koristi za uspešno vođenje krivičnog postupka.

79 Vid. *Ekimdzhiev and others v. Bulgaria*, para. 400–407; *Škoberne v. Slovenia*, para. 142–143.

80 Operatori su u obavezi sa da zadržane podatke *učine dostupnim putem odgovarajućeg tehničkog interfejsa* (čl. 9 st. 2 Pravilnika), odnosno da omoguće tehničko povezivanje svoje opreme sa opremom nadležnih državnih organa upotrebom odgovarajućeg *tehničkog interfejsa kojim se omogućava prenos* određenih komunikacionih podataka (čl. 16 i 21 Pravilnika).

81 *Službeni glasnik RS* 104/09.

82 Vid. *Podchasov v. Russia*, para. 72–75.

koje je preduzeta mera.[83] Međutim, u Srbiji se *lice ne obaveštava* o tome da je na osnovu čl. 286 st. 3 ZKP pristupljeno podacima koji se odnose na njega,[84] ali je zato predviđeno da ima pravo da podnese pritužbu nadležnom sudiji za prethodni postupak (čl. 286 st. 5 ZKP).[85]

Do saznanja da je pristupljeno zadržanim podacima koji se na njega odnose okrivljeni bi mogao da dođe posredno, ostvarivanjem **uvida u spise predmeta**, ali tek nakon saslušanja (čl. 251 st. 1 ZKP). S tim u vezi treba istaći da bi u spis predmeta, osim predloga javnog tužioca i naloga sudije za prethodni postupak, *trebalo da budu uključeni* i zadržani podaci kojima su nadležni organi pristupili – iako nije propisana obaveza policije da dostavi izveštaj o pribavljenim podacima ni sudiji za prethodni postupak, pa ni javnom tužiocu (utvrđena je samo načelna obaveza obaveštavanja javnog tužioca o preduzetim merama i radnjama iz čl. 286 st. 2 i 3 ZKP).

Za ostvarivanje prava lica na koje se odnose zadržani podaci kojima je pristupljeno za potrebe krivičnog postupka, pa i prava na obaveštenost, potencijalno su relevantne odredbe sadržane u *ZZPL*,[86] naročito odredba *o pravu na pristup podacima* (čl. 27) i odredba kojom se *to pravo ograničava* (čl. 28). [87] U vezi sa podnošenjem zahteva rukovaocu za ostvarivanje prava povodom obrade podataka o ličnosti (čl. 27 ZZPL), postavlja se pitanje da li bi uopšte bilo realno očekivati da bi neko lice ako nema nikakva obaveštenja, pa ni posredna saznanja o zadržavanju i pristupu zadržanim podacima koji se na njega odnose, iz preventivnih ili drugih sličnih razloga podnosilo takav

[83] Вид. *Ekimdzhiev and others v. Bulgaria*, пара. 416–417.

[84] U ZKP se pitanje obaveštavanja lica uređuje jedino u vezi sa posebnim dokaznim radnjama (čl. 163 ZKP), ali je upitno da li se to čini na adekvatan način, odnosno u skladu sa praksom ESLJP.

[85] S tim u vezi vid. 4.2.3.

[86] Naročito odredbe kojima se uređuju informisanje i načini ostvarivanja prava lica na koje se odnose podaci kada obradu vrše nadležni organi u posebne svrhe (čl. 21), prava lica da mu se određene informacije stave na raspolaganje ili pruže (čl. 25), pravo na pristup podacima (čl. 27), pravo na brisanje ili ograničenje obrade (čl. 32) te prava da bude obavešten u vezi sa ispravkom ili brisanjem podataka i ograničenjem obrade (čl. 34). Više o načinu ostvarivanja prava fizičkih lica u vezi sa obradom podataka o ličnosti vid. u Kalaba 2023.

[87] Ta ograničenja *ne mogu trajati zauvek i neodređeno* već samo u onoj meri i u onom trajanju dok je to neophodno i srazmerno u demokratskom društvu u odnosu na poštovanje osnovnih prava i legitimnih interesa fizičkih lica čiji se podaci obrađuju, a organi bi morali svoju odluku obrazložiti jasnim razlozima utemeljenim na zakonu. Dalje razmatranje tih pitanja nije predmet rada.

zahtev kako bi došlo do saznanja o tome da li su, koji i na koji način zadržani podaci koji se na njega odnose prikupljeni i obrađivani od nadležnih organa za potrebe krivičnog postupka.[88]

4.2.3. Pravno sredstvo

Obaveštavanje lica na koje se odnose zadržani podaci neophodan je preduslov za ostvarivanje prava na delotvorno pravno sredstvo povodom pristupa zadržanim podacima za potrebe krivičnog postupka. S obzirom na to da lice i ne zna da je prema njemu primenjena mera iz čl. 286 st. 3 – zato što se ne obaveštava o tome da je ostvaren pristup zadržanim podacima koji se na njega odnose – postavlja se pitanje njegovog prava da podnese *pritužbu nadležnom sudiji za prethodni postupak* (čl. 286 st. 5). Ako bi lice i bilo obavešteno ili bi uvidom u spis došlo do saznanja, može se postaviti pitanje na koje bi to okolnosti lice podnelo pritužbu, šta bi se njom tražilo i sl. Takođe, upitno je da li je pritužba delotvorno pravno sredstvo protiv naloga, između ostalog, i iz razloga što je sudija za prethodni postupak kome se podnosi pritužba, taj koji je nalog i izdao, a pored toga nejasno je šta bi sudija povodom pritužbe i mogao da učini. Zbog svega navedenog, ne bi se moglo reći da je ZKP na odgovarajući način uredio pravo na delotvorno pravno sredstvo povodom pristupa zadržanim podacima za potrebe krivičnog postupka.[89]

Povodom pristupa zadržanim podacima za potrebe krivičnog postupka, potencijalno mogu biti relevantne i odredbe ZZPL kojima je predviđeno da lica na koje se odnose podaci, kada obradu vrše nadležni organi u posebne svrhe,[90] mogu ostvariti svoja prava i posredstvom poverenika, u skladu sa njegovim ovlašćenjima propisanim tim zakonom (čl. 35), da se lica na koja se odnose zadržani podaci mogu radi zaštite svojih prava propisanih tim zakonom obratiti pritužbom povereniku (čl. 82), čija odluka podleže kontroli upravnog suda (čl. 83), odnosno tužbom sudu (čl. 84). Pitanje koliko se ta pravna sredstva mogu smatrati delotvornim nije predmet ovog rada.

---

88 Treba napomenuti i to da ZZPL predviđa dva režima obrade podataka o ličnosti – opšti i posebni. Više o opštem i posebnom režimu obrade Milić, Kalaba 2023.

89 Vid. *Ekimdzhiev and others v. Bulgaria*, para. 376–382

90 O poteškoćama da se utvrde subjekti koji se mogu smatrati nadležnim organom koji vrši obradu podataka o ličnosti u posebne svrhe vid. Milić, Kalaba 2024.

4.2.4. „Sudbina" zadržanih podataka

ESLJP je razmatrao kako je uređena sudbina zadržanih podataka kojima su pristupili nadležni organi u situaciji kada nije pokrenut krivični postupak i kada su prikupljeni podaci uključeni u spis krivičnog predmeta.[91] Što se tiče čuvanja, pristupa, ispitivanja, korišćenja, saopštavanja i uništavanja zadržanih podataka kojima su pristupili nadležni organi za potrebe krivičnog postupka, da bi se utvrdilo da li je u Srbiji obezbeđen odgovarajući nivo zaštite, treba uzeti u obzir nekoliko propisa.

ZEK obavezuje operatore da preduzmu određene *mere zaštite*, kojima, između ostalog, treba da se obezbedi da zadržani podaci budu zaštićeni od slučajnog ili nedopuštenog uništenja, slučajnog gubitka ili izmene, neovlašćenog ili nezakonitog čuvanja, obrade, pristupa ili otkrivanja – *u skladu sa ZZPL* (čl. 130 st. 1 tač. 3), i *uništeni* po isteku roka od 12 meseci od dana okončanja komunikacije (čl. 130 st. 1 tač. 4).[92] Takođe, ZEK obavezuje operatore (ne i nadležne organe kome su podaci dostavljeni) da podatke koji su *sačuvani i dostavljeni nadležnim organima* budu zaštićeni od slučajnog ili nedopuštenog uništenja, slučajnog gubitka ili izmene, neovlašćenog ili nezakonitog čuvanja, obrade, pristupa ili otkrivanja, ali tada *u skladu sa ZTP*,[93] dok za uništenje tih podataka, osim što predviđa da se na njih *ne odnosi rok od 12 meseci*, ZEK ne sadrži pravila, već je to uređeno *drugim propisima*. U Srbiji nažalost još uvek ne postoji propis kojim bi se na odgovarajući i sveobuhvatan način uredila pravila o obradi podataka o ličnosti koju vrše *pravosudni organi uopšte*. Mere zaštite zadržanih podataka kojima je pristupila *policija* predviđene su u Zakonu o evidencijama i obradi podataka u oblasti unutrašnjih poslova[94] (Zakon o evidencijama[95]).

I dok ZKP ne sadrži pravilo o tome šta se dešava sa zadržanim podacima kojima je pristupljeno a *krivični postupak nije pokrenut* (npr. nije propisano da se uništavaju u određenom roku pod određenim uslovima),[96] treba imati

---

[91] Vid. *Ekimdzhiev and others v. Bulgaria*, para. 408–409.

[92] Nadzor nad izvršenjem ovih obaveza vrši poverenik (čl. 130 st. 3 ZEK).

[93] Nadzor nad izvršenjem ovih obaveza vrši i Ministarstvo pravde, kao organ nadležan za nadzor nad sprovođenjem ZTP (čl. 130 st. 3 ZEK).

[94] *Službeni glasnik RS* 24/2018.

[95] Čl. 42 koji uređuje evidenciju primenjenih operativnih i operativno-tehničkih sredstava, metoda i radnji, propisano je da Ministarstvo prikuplja i obrađuje podatke u skladu s propisima kojima se uređuje krivični postupak (ZKP) i elektronska komunikacija (ZEK).

[96] Kako to čini izričitom odredbom o postupanju s materijalom koji je prikupljen sprovođenjem posebnih dokaznih radnji (vid. čl. 163 ZKP).

u vidu da u skladu sa Zakonom o evidencijama[97] policija vodi evidenciju o pristupu zadržanim podacima u telekomunikacionom saobraćaju,[98] da ti podaci predstavljaju tajne podatke koji se označavaju u skladu s propisima o tajnosti podataka i da se čuvaju *trajno* (čl. 42 st. 2)[99] – dakle, bez obzira na to da li je krivični postupak pokrenut i kakav je ishod postupka. Upitno je koliko je takvo rešenje u skladu ne samo sa ZZPL nego i sa Direktivom 2016/680, no dalje razmatranje tog pitanja nije predmet našeg rada.

Za sudbinu zadržanih podataka kojima je pristupljeno u slučaju da je **krivični postupak pokrenut** relevantno je pravilo iz ZKP po kojem pojedine spise predmeta može razmatrati, kopirati ili snimati *svako ko ima opravdani interes* da to čini: u toku postupka (pa i predistražnog)[100] – ako to dozvoli javni tužilac,[101] odnosno sud; a nakon završetka postupka – po

---

[97] Čl. 42, koji uređuje evidenciju primenjenih operativnih i operativno-tehničkih sredstava, metoda i radnji, propisuje da Ministarstvo *prikuplja i obrađuje podatke* u skladu s propisima kojima se uređuje krivični postupak (ZKP) i elektronska komunikacija (ZEK).

[98] Evidencija *sadrži podatke iz naredbe* sudije za prethodni postupak nadležnog suda na osnovu koje se vrši pristup zadržanim podacima, a koji *mogu da se odnose na*: ime i prezime lica, ime jednog roditelja, nadimak, JMBG, datum, mesto, opštinu i državu rođenja, adresu prebivališta/boravišta lica, nacionalnost, radno mesto, broj telefona ili IMEI broj telefonskog aparata, korisnički broj, elektronsku adresu, vrstu vozila i uređaja, registarsku oznaku vozila, koji su obuhvaćeni naredbom suda, odnosno podatke potrebne za praćenje i utvrđivanje izvora komunikacije, utvrđivanje odredišta komunikacije, utvrđivanje početka, trajanja i završetka komunikacije, utvrđivanje vrste komunikacije, identifikaciju terminalne opreme korisnika, utvrđivanje lokacije mobilne terminalne opreme korisnika (čl. 42 st. 1).

[99] Iako je u čl. 42 st. 3 i 4 tog zakona propisano da Ministarstvo *do zastarelosti krivičnog gonjenja* čuva podatke koji se obrađuju u skladu sa ZKP, u sklopu dužnosti preduzimanja potrebnih mera i radnji da se pronađe učinilac krivičnog dela, da se učinilac ili saučesnik ne sakrije ili ne pobegne, da se otkriju i obezbede tragovi krivičnog dela i predmeti koji mogu poslužiti kao dokaz i prikupljanja svih obaveštenja koja bi mogla biti od koristi za uspešno vođenje krivičnog postupka – odnosno u skladu s čl. 286 ZKP, *među kojima je pribavljanje evidencije* iz čl. 286 st. 3–5 ZKP – st. 2 istog člana *posebno i na bitno drugačiji način* uređuje rok čuvanja evidencije o pristupu zadržanim podacima (a time i rok čuvanja zadržanih podataka koji se unose u evidenciju).

[100] S obzirom na značenje izraza „postupak" u smislu čl. 2 st. 2 tač. 14) ZKP.

[101] S tim u vezi, treba naglasiti da javni tužilac prilikom davanja dozvole za razmatranje spisa ili predmeta, odnosno izdavanja fotokopije spisa, čak i licima koja imaju opravdani interes, *vodi računa o fazi u kojoj se nalazi postupak po predmetu i o interesima redovnog odvijanja postupka* (čl. 65 Pravilnika o upravi u javnim tužilaštvima, *Službeni glasnik RS* 110/2009, 87/2010, 5/2012, 54/2017, 14/2018 i 57/2019). Takođe, odredbama ZKP je propisano da se razmatranje spisa može rešenjem uskratiti ili usloviti zabranom javne upotrebe imena učesnika u postupku, ukoliko bi pravo na privatnost moglo da bude teže povređeno (čl. 250 st. 3 ZKP).

odobrenju predsednika suda ili službenog lica koje on odredi (čl. 250 ZKP).[102] Razmatranje spisa je *ograničeno* samo u slučaju da *imaju oznaku stepena tajnosti* – međutim, za razliku od posebnih dokaznih radnji, podaci o predlaganju, odlučivanju i sprovođenju mere iz čl. 286 st. 3 ne predstavljaju tajne podatke niti je u ZKP izričito propisano da se predlog javnog tužioca, nalog sudije za prethodni postupak i izveštaj o prikupljenim podacima označavaju oznakom stepena tajnosti, u skladu sa propisima kojima se uređuju tajni podaci. Imajući u vidu da je ESLJP našao da se *ne može prihvatiti da postoji odgovarajući nivo zaštite zadržanih podataka*,[103] kada se uključuju i čuvaju u spise predmeta i prate njegovu sudbinu, pa im može pristupiti svako ko ima pristup samom spisu, trebalo bi se osvrnuti na uređenje tog pitanja u Srbiji.

4.2.5. Nadzor

Što se tiče nadzora nad ostvarivanjem pristupa zadržanim podacima, upitno je da li i u kojoj meri postojeći mehanizam Srbiji može da obezbedi da se ovlašćenja za pristup ne zloupotrebljavaju.

Inspekcijski nadzor nad primenom ZEK i propisa kojima se uređuje delatnost elektronskih komunikacija obavlja Ministarstvo informisanja i telekomunikacija, posredstvom inspektora elektronskih komunikacija (čl. 163 ZEK 2023).[104] Međutim, inspektor *nije nadležan* da vrši nadzor *nad ostvarivanjem pristupa nadležnih organa*, tim pre ni da ocenjuje opravdanost ostvarivanja pristupa zadržanim podacima u konkretnom slučaju. Osim toga, *nadzorom nad izvršenjem obaveza* da se preduzmu određene *mere zaštite* zadržanih podataka (čl. 130 st. 3 ZEK) *nije obuhvaćen* nadzor nad postupanjem nadležnih organa.

---

[102] Spisi pravnosnažno okončanog krivičnog postupka se čuvaju u skladu sa Sudskim poslovnikom (*Službeni glasnik RS* 110/2009, 70/2011, 19/2012, 89/2013, 96/2015, 104/2015, 113/2015, 39/2016, 56/2016, 77/2016, 16/2018, 78/2018, 43/2019, 93/2019 i 18/2022), kojim se uređuju način arhiviranja i rokovi čuvanja arhiviranog predmeta u krivičnom postupku, računajući od dana pravnosnažnosti postupka, a zavisno od ishoda postupka (naročito, s obzirom na vrstu i visinu izrečene sankcije).

[103] Vid. *Ekimdzhiev and others v. Bulgaria*, para. 408–409.

[104] Inspektor je, osim ovlašćenja iz zakona kojim se uređuje obavljanje poslova inspekcije, ovlašćen, između ostalog, da proverava postupanje privrednog subjekta u vezi sa primenom mera zaštite podataka o ličnosti i privatnosti (čl. 166 st. 1 t. 6 ZEK 2023), te postupanje operatora u vezi sa omogućavanjem pristupa zadržanim podacima (čl. 166 st. 1 t. 7 ZEK 2023). Ukoliko se u vršenju inspekcijskog nadzora utvrde nezakonitosti u primeni propisa, inspektor je ovlašćen da naloži određene mere.

Povodom *kontrole ostvarivanja pristupa* zadržanim podacima *na osnovu evidencija* koje vode operatori i nadležni organi, u pogledu evidencija koje se vode *na osnovu čl. 128 st. 8 i 9 ZEK*, s obzirom na to da se čuvaju kao tajna, opoziv tajnosti podatka, odnosno dokumenta koji sadrži tajni podatak bio bi moguć samo u slučajevima, na način i pod uslovima koji su propisani odredbama ZTP. *Evidencije o zahtevima za pristup zadržanim podacima iz čl. 130a ZEK*, koje se jednom godišnje dostavljaju povereniku, sadrže samo sumarni broj zahteva za pristup i ostvarenih pristupa – štaviše, izričito je propisano da ne sadrže podatke o ličnosti čijim podacima se pristupalo (čl. 130a st. 3 ZEK).[105] Na taj način je ograničena (ali ne i isključena) mogućnost poverenika da vrši efektivnu kontrolu postupanja operatora *u pojedinim slučajevima*, s obzirom na ovlašćenja koja ima, prvenstveno *u smislu ZZPL*. Drugo je pitanje da li su ta ovlašćenja adekvatno propisana i da li se mogu na efikasan način koristiti u praksi.

U pogledu „nadzornog mehanizma" u okviru ZKP, sudija za prethodni postupak koji je izdao nalog nije u poziciji da kontroliše ostvarivanje pristupa ni korišćenje zadržanih podataka kojima je pristupljeno. Naime, o pristupu zadržanim podacima policija odmah, a najkasnije u roku od 24 časa nakon preduzimanja, obaveštava javnog tužioca (čl. 286 st. 4), a ne sudiju. Pri tome treba imati u vidu da se, prema prikazanoj praksi Suda pravde EU i ESLJP, javni tužilac ne može smatrati organom koje ispunjava uslove nezavisnosti koji se zahtevaju za organ nadležan za obavljanje nadzora nad pristupom zadržanim podacima, s pravom se može postaviti pitanje adekvatnosti domaćeg rešenja. ZKP ne zahteva da se sudiji dostavi bilo kakav izveštaj o ostvarivanju

[105] Problem koji se odnosi na dostavljanje pomenutih evidencija povereniku već nekoliko godina je predmet analize nekoliko nevladinih organizacija koja se bave tematikom privatnosti podataka, digitalne bezbednosti i transparentnosti rada organa vlasti. U svojim izveštajima i analizama ukazuju na to da, osim značajnog pada transparentnosti izveštavanja operatora i nadležnih organa kada je reč o njihovim praksama pristupa zadržanim podacima, što se najviše ogleda u propuštanju da se dostave informacije o samostalnom pristupu podacima, problem predstavljaju i vidljive razlike u izveštajima. Takođe, ističe se da je, kako članom 130a ZEK nije dovoljno precizno uređena sadržina evidencije koja se dostavlja povereniku, prostor za proizvoljno tumačenje te pravne obaveze prilično širok i deluje da zavisi od dobre volje ili, u najboljem slučaju, od procedura uspostavljenih na korporativnom nivou konkretnog pružaoca usluga elektronskih komunikacija. Praksa bi se možda promenila ukoliko bi se izmenama zakona ili odgovarajućim podzakonskim aktom (npr. pravilnikom) propisao obavezujući obrazac za dostavljanje evidencije o zadržanim podacima, čiji bi elementi morali da sadrže uniformne informacije. Trenutne prakse operatora i nadležnih organa više predstavljaju formalno ispunjenje obaveze nego suštinsku intenciju da se zakonom propiše mehanizam transparentnosti zadržavanja podataka o elektronskim komunikacijama i pristupanja tim podacima. Share fondacija, Pregled evidencije pristupa zadržanim podacima u Srbiji za 2020, 2018. i 2017. godinu.

pristupa niti da bude obavešten o uništavanju irelevantnih ili beskorisnih komunikacionih podataka kojima je pristupljeno. Što se tiče eventualnog reagovanja sudije povodom pritužbe lica čijim podacima se pristupilo (u smislu čl. 286 st. 5) nejasno je koja bi bila njegova ovlašćenja.

5. ZAKLJUČAK

U Srbiji su operatori obavezni da masovno zadržavaju i čuvaju 12 meseci od ostvarene komunikacije ogroman broj podataka o svim elektronskim komunikacijama svih svojih korisnika. Obavezu masovnog, neselektivnog zadržavanja i čuvanja zadržanih podataka ZEK je propisao ne opravdavajući je bilo kakvom jasnom svrhom i ciljem. S druge strane, prema ZEK, pristup je dozvoljen izuzetno – samo „na određeno vreme" i „na osnovu odluke suda" ako je to „neophodno" radi vođenja krivičnog postupka ili zaštite bezbednosti Republike Srbije, a na način predviđen drugim zakonom. Pristup podacima koji su zadržani na osnovu ZEK ostvaruje se za potrebe krivičnog postupka na osnovu ZKP, no tim propisom to pitanje nije uređeno na odgovarajući način.

Domaćem pravnom okviru su stoga upućene kritike zbog potencijalne neusklađenosti sa Ustavom i neusaglašenosti sa EKLJP i pravom EU. Treba voditi računa o tome da je Srbija, kao članica Saveta Evrope i kao kandidat za članstvo u EU, dužna da propise i njihovu primenu uskladi s pravom tih međunarodnih organizacija, a što do sada, čini se, nije učinila u dovoljnoj meri i na odgovarajući način. Autori u radu jasno ukazuju na te neusaglašenostima, upućujući na relevantne odluke Suda EU i ESLJP.

Iz prakse Suda EU jasno proizlazi da se opšte i neselektivno zadržavanje komunikacionih podataka, kakvo propisuje ZEK, ne može samo po sebi opravdati te da je protivno pravu EU. U pogledu pristupa zadržanim podacima od nadležnih organa za potrebe krivičnog postupka, ne bi se moglo smatrati da je pravno uređenje u ZKP ograničeno na ono što je strogo neophodno „u demokratskom društvu". Zbog svega navedenog u radu, nakon analize relevantne prakse Suda pravde EU, ne bi se moglo reći da su do sada uzeti u obzir stavovi i smernice utvrđeni u odlukama najvišeg suda EU, a bilo bi poželjno da ih zakonodavac razmotri.

Što se tiče usaglašenosti domaćih propisa sa EKLJP, iz prakse ESLJP proizlazi da, s obzirom na to da pribavljanje komunikacionih podataka putem masovnog i opšteg zadržavanja i pristupa zadržanim podacima može biti jednako nametljivo kao i masovno prikupljanje sadržaja komunikacija, opšte zadržavanje komunikacionih podataka od pružalaca komunikacionih

usluga i pristup nadležnih organa tim podacima u pojedinačnim slučajevima moraju biti praćeni, *mutatis mutandis*, istim merama zaštite kao i tajni nadzor komunikacije. Da se pred ESLJP pokrene postupak protiv Srbije zbog kršenja prava iz EKLJP u vezi sa zadržavanjem podataka i pristupom zadržanim podacima za potrebe krivičnog postupka, nije isključeno da bi ESLJP, kao u slučaju Slovenije, našao da postojeće odredbe, koje predstavljaju osnov za zadržavanje i čuvanje komunikacionih podataka, ne ispunjavaju uslov „kvaliteta zakona" i da ne mogu da ograniče „mešanje" u prava iz člana 8 EKLJP na ono što je „neophodno u demokratskom društvu", a da su zadržavanje, naknadni pristup i obrada komunikacionih podataka na osnovu takvog pravnog okvira u suprotnosti sa Konvencijom. Takođe, može se pretpostaviti sa visokim stepenom verovatnoće da bi ESLJP nesumnjivo ukazao Srbiji, kao što je to učinio i u slučaju Bugarske, na to da treba da izvrši neophodne izmene u domaćem pravnom okviru kako bi okončala kršenje prava i obezbedila da njeni propisi budu kompatibilni sa Konvencijom.

LITERATURA

[1] Bugarski, Tatjana, Milana Pisarić. 4/2020. Zadržavanje podataka u praksi Suda Evropske Unije. *Zbornik Pravnog fakulteta u Novom Sadu* 54: 1231–1252.

[2] Kalaba, Ostoja. 2023. Obrada podataka o ličnosti od strane crkava i verskih zajednica u pravu i praksi EU i Republike Srbije. 867–896. *Savremeno državno-crkveno pravo*, ur. Vladimir Đurić, Dalibor Đukić. Beograd – Budva: Institut za uporedno pravo – Mitropolija crnogorsko-primorska SPC:

[3] Milić, Ivan, Ostoja Kalaba. 2023. Savremeni 'pametni' sistemi za regulisanje saobraćaja u gradovima Republike Srbije – (ne)usklađenost pozitivnopravnih propisa („pazi, snima se"). 253–275. *Pravo između ideala i stvarnosti*, ur. Strahinja Miljković. Kosovska Mitrovica: Pravni fakultet Univerziteta u Prištini sa privremenim sedištem u Kosovskoj Mitrovici, Institut za uporedno pravo.

[4] Milić, Ivan, Ostoja Kalaba. 2024. Prekršajna odgovornost i kazne za kršenje zakona o zaštiti podataka o ličnosti. 237–267. *Dinamika savremenog pravnog poretka*, ur. Srđan Radulović. Kosovska Mitrovica: Pravni fakultet Univerziteta u Prištini sa privremenim sedištem u Kosovskoj Mitrovici – Institut za uporedno pravo – Institut za kriminološka i sociološka istraživanja.

[5] Mitsilegas, Valsamis, Elspeth Guild, Elif Kuskonmaz, Niovi Vavoula. 1–2/2023. Data retention and the future of large-scale surveillance: The evolution and contestation of judicial benchmarks. *European Law Journal* 29: 176–211.

[6] Pisarić, Milana. 2019. *Elektronski dokazi u krivičnom postupku*. Novi Sad: Pravni fakultet u Novom Sadu.

[7] Podkowik, Jan, Robert Rybski, Marek Zubik. 5/2021. Judicial dialogue on data retention laws: A breakthrough for European constitutional courts? *International Journal of Constitutional Law* 19: 1597–1631.

[8] Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti. 2012. Izveštaj o izvršenom nadzoru nad sprovođenjem i izvršavanjem Zakona o zaštiti podataka o ličnosti od strane operatora mobilne i fiksne telefonije u Republici Srbiji. *https://labs.rs/Documents/PoverenikovIzvestaj.pdf*, poslednji pristup 9. april 2024.

[9] Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti. 2013. Izveštaj o sprovođenju Zakona o slobodnom pristupu informacijama od javnog značaja i Zakona o zaštiti podataka o ličnosti za 2012. godinu. *https://www.poverenik.rs/images/stories/dokumentacija-nova/izvestajiPoverenika/2012/latizvestaj2012final.pdf*, poslednji pristup 9. april 2024.

[10] Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti. 2015. Izveštaj o izvršenom nadzoru nad sprovođenjem i izvršavanjem Zakona o zaštiti podataka o ličnosti od strane operatora elektronskih komunikacija koji pružaju usluge pristupa internetu i internet usluge. *https://www.poverenik.rs/sr-yu/saopstenja/2128-nuzno-je-popravljati-nivo-zastite-licnih-podataka-u-oblasti-elektronskih-komunikacija.html*, poslednji pristup 9. april 2024.

[11] Share fondacija. Pregled evidencije pristupa zadržanim podacima u Srbiji za 2020. godinu. *https://www.sharefoundation.info/wp-content/uploads/Zadrzani-podaci-2020_izvestaj.pdf*, poslednji pristup 9. april 2024.

[12] Share fondacija. Pregled evidencije pristupa zadržanim podacima u Srbiji za 2018. godinu. *https://www.sharefoundation.info/sr/pristup-bez-transparentnosti-praksa-zadrzavanja-podataka-u-2018/*, poslednji pristup 9. aprila 2024.

[13] Share fondacija. Pregled evidencije pristupa zadržanim podacima u Srbiji za 2017. godinu. *https://resursi.sharefoundation.info/sr/resource/zadrzavanje-podataka-o-komunikaciji-u-srbiji-koliko-smo-pod-nadzorom/*, poslednji pristup 9. april 2024.

[14] *Washington Post*. 2014. Transcript of President Obama's Jan. 17 speech on NSA reforms. January 17. *https://www.washingtonpost.com/politics/full-text-of-president-obamas-jan-17-speech-on-nsa-reforms/2014/01/17/fa33590a-7f8c-11e3–9556–4a4bf7bcbd84_story.html*, poslednji pristup 24. decembar 2023.

Milana M. PISARIĆ, PhD

Assistant Professor, University of Novi Sad Faculty of Law, Serbia

Ostoja S. KALABA, LL.M.

Advisor at the Office of the Commissioner for Information of Public Importance and Personal Data Protection, PhD student, Serbia

DATA RETENTION AND CRIMINAL PROCEDURE IN SERBIA

Summary

The use of information technology enables state authorities to prosecute perpetrators and process personal data on an unprecedented scale and in an unimaginable way, in the course of taking measures and actions to prevent, detect and investigate criminal acts. One of the disputed processing is the nonselective mass monitoring of electronic communications in the form of retention of communication data, which, given the technological development and social importance of electronic communications, can on occasion reveal more about an individual than the content of the communication itself. This form of data processing represents interference with guaranteed human rights and freedoms, and need to be legally regulated in order to prevent their violation. The authors analyze the legal framework for retention of communication data and access to retained data for the purposes of criminal proceedings in Serbia, especially in light of the relevant practices of the CJEU and ECtHR.

Key words: *Electronic communications. – Data retention. – Criminal procedure. – Personal data protection. – Privacy*.

Article history:
Received: 10. 4. 2024.
Accepted: 29. 11. 2024.