MEĐUNARODNOPRAVNE IMPLIKACIJE MASOVNOG NADZORA ELEKTRONIČKIH KOMUNIKACIJA U KONTEKSTU LJUDSKIH PRAVA, S POSEBNIM OSVRTOM NA SIGURNOSNO-OBAVJEŠTAJNI SUSTAV U REPUBLICI HRVATSKOJ

Izvorni znanstveni rad

UDK 004.3/.4
342.721
355.401(497.5)
341.231.14
341.645.5(4)

Primljeno: 13. veljače 2017.

Zrinka Salaj*

Cilj je ovog rada izložiti međunarodnopravne implikacije mirnodopske špijunaže u obliku masovnog elektroničkog nadzora komunikacija. Pitanje je to koje se aktualiziralo objavom otuđenih državnih tajnih dokumenata koji su razotkrili obujam masovnog nadzora svjetskih elektroničkih komunikacija od strane država, koje su to činile zlouporabljujući tehničke karakteristike prijenosa komunikacija te iskorištavajući nedostatke međunarodnopravnog uređenja mirnodopske špijunaže.

U radu se analizira ključno pitanje koje za sobom povlači masovni elektronički nadzor komunikacija, a to su međunarodnopravne posljedice spram pojedinca koji je meta nadzora i odnosa koji se uspostavlja između njega i države koja nadzor obavlja, a koji je u domeni ljudskih prava. U tom smislu ispituje se praksa međunarodnih mehanizama za zaštitu ljudskih prava, poglavito Europskog suda za ljudska prava (Europske komisije za ljudska prava), s kojom se potom uspoređuje pravni okvir hrvatskog sigurnosno-obavještajnog sustava kako bi se utvrdilo zadovoljava li on zahtjeve zakonitosti i zabrane samovolje u ograničavanju prava na privatnost.

Ključne riječi: masovni elektronički nadzor, pravo na privatnost, hrvatski sigurnosno-obavještajni sustav

1. UVOD

Službeni tajni dokumenti koje je 2013. godine svjetskoj javnosti putem medija učinio dostupnima Edward Snowden, bivši analitičar američke Nacionalne sigurnosne agencije [NSA], prouzročili su geopolitički i međunarodnopravni potres bez presedana, a Snowdena prometnuli u najpoznatijeg svjetskog zviždača, iako ne i prvog koji je na svjetlo dana izložio rad NSA-a.[1] Naime dokumenti su razotkrili javnosti dotad nepoznat opseg i

* Zrinka Salaj, Ministarstvo pravosuđa Republike Hrvatske, polaznica Poslijediplomskog doktorskog studija iz međunarodnog javnog i privatnog prava na Pravnom fakultetu Sveučilišta u Zagrebu

[1] The Guardian's Audio Long Reads, *How the Pentagon punished NSA whistleblowers,* 3. lipnja 2016., dostupno na: https://www.theguardian.com/news/audio/2016/jun/03/how-the-pentagon-punished-nsa-whistleblowers (pristup 6. veljače 2017.).

metode sustava globalnog i masovnog elektroničkog nadzora svjetskih elektroničkih komunikacija od strane američkih i britanskih državnih agencija. Navedeni događaj izazvao je salve reakcija, ali i konkretnih akcija Ujedinjenih naroda,[2] Europskog parlamenta,[3] stranih vođa[4] i međunarodnih korporacija[5] te na kraju samih Sjedinjenih Američkih Država, čija je praksa bila razotkrivena.[6] Neke od reakcija, poglavito europskih institucija, imale su za cilj pozivanje na pružanje zaštite (pravne i političke)[7] zviždačima kao što je Snowden i isticale su da je djelovanje zviždača najdjelotvornije sredstvo za provođenje ograničenja obavještajnog nadzora,[8] odnosno protiv kršenja ljudskih prava.

Ujedinjeno Kraljevstvo i SAD zasigurno su države koje zbog svoje ekonomske moći prednjače u mogućnostima masovnog nadzora. Međutim i druge države koriste tok elektroničkih komunikacija kroz svoje područje kako bi ih neometano pratile i sakupljale. Primjerom upravo Ujedinjenog Kraljevstva, ali i Njemačke, Rusije i Mađarske, bavio se i Europski sud za ljudska prava [ESLJP],[9] dok globalno istraživačko novinarstvo i medijski *outleti* za objavu tajnih dokumenata koji su „procurili" u javnost od strane zviždača i hakera, kao što je *Wikileaks*, daju primjere oko 25 država koje čine isto.[10]

Čak su i Ujedinjeni narodi izrazili zabrinutost zbog politika i praksa sve većeg broja država koje iskorištavaju ranjivost digitalnih komunikacija te uvode masovni nadzor ne kao „iznimnu mjeru", nego kao „opasnu naviku",[11] ističući posebno suradnju između država i

---

[2] UNGA, *The Right to Privacy in the Digital Age*, UN Doc. A/C.3/68/L.45/Rev.1, 20. studenog 2013.; UNGA, *Resolution on the Right to Privacy in the Digital Age*, G.A. Res 68/167, UN Doc. A/RES/68/, 21. siječnja 2016., 167; UNGA, *The Right to Privacy in the Digital Age,* UN Doc A/C.3/71/L.39/Rev.1, 16. studenog 2016.

[3] Europski parlament, Rezolucija o suspenziji Sporazuma o Programu za praćenje financiranja terorističkih djelatnosti (TFTP) zbog nadzora američke Agencije za nacionalnu sigurnost, Rezolucija 2013/2831(RSP) od 23. listopada 2013.

[4] Bloomberg News, *German government cancels Verizon Communications Inc deal in wake of NSA spy scandal*, 27. srpnja 2014., dostupno na: http://www.financialpost.com/m/wp/blog.html?b=business.financialpost.com/2014/06/27/german-government-cancels-verizon-communications-inc-deal-in-wake-of-nsa-spy-scandal (pristup 6. veljače 2017.).

[5] Otvoreno pismo Senatu u vezi s *USA Freedom Act*, potpisano od strane *AOL*-a, *Applea*, *Dropboxa*, *Evernotea*, *Facebooka*, *Googlea*, *Linkedina*, *Microsofta*, *Twittera*, *Yahooa*: *Global Government Surveillance Reform*, prosinac 2013.; svibanj 2015., dostupno na: https://www.reformgovernmentsurveillance.com/ (pristup 6. veljače 2017.).

[6] The White House, Office of the Press Secretary, *Remarks by the President on Review of Signals Intelligence,* 17. siječnja 2014*.,* https://www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence (pristup 6. veljače 2017.) [*Govor Obama*]; *The President's Review Group on Intelligence and Communications Technologies*: Richard A. Clarke, Michael J. Morell, Geoffrey R. Stone, Cass R. Sunstein & Peter Swire, *The NSA Report: Liberty and Security in a Changing World*, 12. prosinca 2013., dostupno na: http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf. (pristup 7. prosinca 2016.).

[7] Europski parlament, *Rezolucija o programu nadzora Agencije za nacionalnu sigurnost SAD-a (NSA), nadzornim tijelima u različitim državama članicama i njihovu utjecaju na temeljna prava građana EU-a te o transatlantskoj suradnji u pravosuđu i unutarnjim poslovima*, Rezolucija broj 2013/2188 od 12. ožujka 2014.; Parlamentarna skupština Vijeća Europe, *Improving the protection of whistle-blowers,* Rezolucija 2060 (2015) od 23. lipnja 2015.

[8] *Id.*

[9] Vidi *infra* dio 2.

[10] Wikileaks, *The Spy Files*, https://wikileaks.org/the-spyfiles.html (pristup 1. prosinca 2016.).

[11] Odbor za prava čovjeka, *Izvještaj o pravu na privatnost Ureda Visokog povjerenika za ljudska prava* (A/HRC/27/37), 30. lipnja 2014. [*Izvještaj*], para. 20, str. 3.

privatnih kompanija u izvršavanju takva nadzora.[12] Naime osim sustava masovnog nadzora podataka putem vlastitih infrastruktura,[13] koji neselektivno sakuplja podatke, koji se potom analiziraju od strane ovlaštenih osoba po određenom ključu,[14] države sve češće posežu za podacima koje privatne kompanije imaju o svojim klijentima. Najčešće se radi o kompanijama koje pružaju telekomunikacijske usluge. U tu svrhu države uspostavljaju programe koji im pružaju izravan pristup tim podacima.[15]

Navedene prakse razotkrivaju stvarnu ranjivost svih meta takva načina praćenja, ali i njihovu međunarodnopravnu ranjivost, odnosno nezaštićenost, poglavito kada se radi o privatnim osobama izvan teritorija države koja obavlja nadzor. U izostanku kvalitetne akcije države da zaštiti prava kako svojih državljana tako i stranaca pojedinci se već okreću dostupnim međunarodnim mehanizmima za zaštitu svojih ljudskih prava.

2. MASOVNI ELEKTRONIČKI NADZOR U KONTEKSTU LJUDSKIH PRAVA

Pravo na privatnost predstavlja temeljno ljudsko pravo, priznato i zaštićeno gotovo svim relevantnim dokumentima za zaštitu ljudskih prava.[16] Presretanje i nadzor komunikacije pojedinca samo po sebi predstavlja ograničavanje uživanja njegova prava na privatnost. Istovremeno, navedeni dokumenti priznaju i ograničavanje prava na privatnost od strane države sve dok su ta ograničenja zakonita i nearbitrarna.[17]

Neupitna je obveza država stranaka međunarodnih instrumenata za zaštitu ljudskih prava da navedena prava osiguraju i jamče „svim osobama na svom području i područjima koja se nalaze pod njenom jurisdikcijom“, kako to navodi članak 2. stavak 1. Međunarodnog pakta o građanskim i političkim pravima, instrumenta za zaštitu ljudskih

[12] *Id.*

[13] Europski parlament, *Izvješće o postojanju globalnog sustava za presretanje privatne i komercijalne komunikacije (Sustav za presretanje ECHELON*) (2001/2098(INI)), 11. srpnja 2001., str 134; Europski parlament, *Rezolucija Europskog parlamenta od 29. listopada 2015. o daljnjem postupanju nakon usvajanja Rezolucije Europskog parlamenta o elektroničkom masovnom nadzoru građana EU-a 12. ožujka 2014*. (2015/2635(RSP)).

[14] Foreign Intelligence Surveillance Court, *Amended Memorandum Opinion*, Docket Number: 13-109 od 29. kolovoza 2013., str. 5, dostupno na: https://www.aclu.org/files/assets/br13-09-primary-order.pdf (pristup19. siječnja 2017.).

[15] Ira Rubenstein, Greg Nojeim, Ronald Lee, *Systematic Government Access to Personal Data, a comparative analysis*, 4 *International Data Privacy Law* 13 (2014), str. 96-119; [*Rubenstein i dr*.]; Bruno Magrani, *Systematic Government access to private-sector data in Brazil,* 4 International Data Privacy Law (2014) 30-38; Sunil Abraham, Elonnai Hickok, *Government access to private-sector data in India,* 2 International Data Privacy Law (2012) 302-315.

[16] *Opća deklaracija o ljudskim pravima,* usvojena i proglašena od Opće skupštine Rezolucijom 217 A (III) 10. prosinca 1948., (NN (Međunarodni dio)12/2009), [*Opća deklaracija*] čl. 12.; *Međunarodni pakt o građanskim i političkim pravima* (NN MU 7/2005), [MPGPP] čl. 17.; *Europska konvencija za zaštitu ljudskih prava i temeljnih sloboda*, pročišćeni tekst (NN MU 18/97, 6/99, 14/02, 13/03, 9/05, 1/06, 2/10), [EKLJP] čl. 8.; Organizacija američkih država, *Američka konvencija o pravima čovjeka, "Pakt iz San Josea", Kostarika*, od 22. studenog 1969., 1144 UNTS 123, čl. 11.; Liga arapskih država, *Arapska povelja o ljudskim pravima* od 22. svibnja 2004. godine, 12 Int'l Hum. Rts. Rep. 893 (2005), čl. 21.

[17] *Izvještaj,* str. 7-9: Odbor za prava čovjeka, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye,* UN Doc. A/HRC/29/32, 22. svibnja 2015., § 29-35.

prava s najviše ratifikacija (više od 165).[18] Međutim tehnička složenost masovnog elektroničkog nadzora omogućuje praćenje komunikacija pojedinaca koji se ne nalaze na području države koja vrši nadzor s obzirom na to da takva vrsta nadzora iskorištava prednosti infrastruktura koje omogućuju globalne komunikacijske tokove podatkovnog prometa. Stoga se postavlja pitanje ekstrateritorijalne primjene tih međunarodnih ugovora, odnosno opsega zaštite koja je osigurana pojedincima čiju komunikaciju omogućuju upravo navedene infrastrukture, a koji nisu stanovnici područja države koja nadzor obavlja.

2.1. Ekstrateritorijalna primjena međunarodnih instrumenata za zaštitu ljudskih prava

S obzirom na to da je pitanje ekstrateritorijalne primjene međunarodnih ugovora namijenjenih zaštiti ljudskih prava osporavano od većeg broja država,[19] upravo se na argument ekstrateritorijalne neprimjenjivosti međunarodnih instrumenata za zaštitu ljudskih prava države pozivaju u argumentiranju legalnosti svoje prakse masovnog elektroničkog praćenja.[20] Iz te činjenice razvidno je da masovna elektronička praćenja iskorištavaju nedovoljnu pravnu zaštićenost stranih privatnih komunikacija.[21]

Pitanje ekstrateritorijalne primjene instrumenata za zaštitu ljudskih prava, poglavito MPGPP-a te EKLJP-a, bilo je razmatrano od strane Međunarodnog suda,[22] Odbora za ljudska prava[23] te ESLJP-a.[24]

Međunarodni je sud u svojem *Savjetodavnom mišljenju o gradnji zida na Okupiranom palestinskom području* utvrdio da se MPGPP primjenjuje ekstrateritorijalno u slučajevima kada vojne snage određene države fizički okupiraju neko područje kroz duže vrijeme.[25]

---

[18] Ured visokog povjerenika za prava čovjeka, *Status Of Ratification Interactive Dashboard*, dostupna na: http://indicators.ohchr.org/ (pristup 9. prosinca 2016.).

[19] United States Department of State, Office of the Legal Adviser, *Memorandum Opinion On The Geographic Scope Of The International Covenant On Civil And Political Rights*, 19. listopada 2010. godine, str. 4, dostupno na: https://www.justsecurity.org/wp-content/uploads/2014/03/state-department-iccpr-memo.pdf (7. prosinca 2016.); Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, UN Doc. A/HRC/23/40, 17. travnja, 2013., § 64; Ashley Deeks, *An International Legal Framework for Surveillance*, 55 VA. J. INT'L L. 291 (2015) [*Deeks*], bilješka 56.

[20] *Id.*

[21] *Govor Obama.*

[22] *Pravne posljedice izgradnje zida na Okupiranom palestinskom području,* Savjetodavno mišljenje, ICJ Reports 2004, 136, § 111.

[23] Odbor za prava čovjeka, General Comment 31, *Nature of the General Legal Obligation on States Parties to the Covenant*, UN Doc. CCPR/C/21/Rev.1/Add.13 (2004), 29. ožujka 2004.; *Sergio Euben Lopez Burgos protiv Urugvaja*, Komunikacija broj R.12/52, UN Doc. Dodatak br. 40 (A/36/40), str. 176 (1981) [*Lopez Burgos*].

[24] *Banković i drugi protiv Belgije i drugih* (odluka), br. ESLJP (2001), § 71; *Issa i drugi protiv Turske* (presuda), br. 31821/96, ESLJP (2004), § 58; *Al-Skeini i drugi protiv Ujedinjenog Kraljevstva* (presuda), br. 55721/07, ESLJP (2011) [*Al-Skeini*], §§ 133-137.

[25] *Pravne posljedice izgradnje zida na Okupiranom palestinskom području,* Savjetodavno mišljenje, ICJ Reports 2004, 136, § 111; *Oružane aktivnosti na teritoriju Konga (Demokratska Republika Kongo protiv Ugande*), ICJ Reports 2005, 168.

ESLJP je u predmetu *Al-Skeini i drugi protiv Ujedinjenog Kraljevstva* bio na istom tragu ustvrđujući da se EKLJP primjenjuje ekstrateritorijalno u slučajevima upotrebe sile od strane agenata države, vojne akcije i vojne okupacije.[26] Nadalje, Odbor za ljudska prava u predmetu *Lopez Burgos protiv Urugvaja* istaknuo je kako bi tumačenje MPGPP-a na način da dopušta državi da krši ljudska prava izvan svojih granica bilo nerazumno.[27] Iz navedenih primjera proizlazi da se za ekstrateritorijalnu primjenu i obvezivost instrumenata za zaštitu ljudskih prava traži određena fizička i faktična kontrola države nad područjem,[28] odnosno nad pojedincem,[29] kao i njezino djelovanje izvan granica svoje jurisdikcije.[30] ESLJP, čija praksa obiluje predmetima u vezi s ekstrateritorijalnom primjenom EKLJP-a, potvrdio je takvu ograničenu ekstrateritorijalnu primjenu instrumenta za zaštitu ljudskih prava samo na situacije u kojima država ima *efektivnu kontrolu* nad područjem ili pojedincem.[31]

Možemo primijetiti da u slučaju elektroničkog praćenja izostaje element efektivne fizičke kontrole nad pojedincem jer je prostorni element elektroničkog praćenja u uvjetima koje osigurava moderna tehnologija zapravo i bespredmetan s obzirom na to da se praćenje izvršava bez obzira na lokaciju pojedinca, odnosno bez potrebe efektivne fizičke kontrole nad pojedincem kakva se zahtijeva za ekstrateritorijalnu primjenu međunarodnih instrumenata.[32] Međutim ono na što se u kontekstu elektroničkog praćenja stavlja naglasak jesu upravo infrastrukture koje državama omogućuju elektronički nadzor.[33] Teško bi bilo osporiti tvrdnju da države nemaju efektivnu kontrolu nad infrastrukturama koje su same upogonile, a koje su platforme kršenja prava na privatnost *en masse*. Također, može se pretpostaviti da se pohrana i analiza tako sakupljenih podataka obavlja na području dotične države, što učvršćuje argument. Nadalje, određeni autori, upravo uzimajući u obzir posebnosti digitalnog doba, izjednačuju fizičku efektivnu kontrolu s *virtualnom* efektivnom kontrolom.[34]

[26] *Al-Skeini*, §§ 133-137.
[27] *Lopez Burgos,* § 12.3. U predmetu se radilo o otmici, nečovječnom postupanju i mučenju državljana Urugvaja počinjenih od strane državnih agenata Urugvaja na području Argentine.
[28] *Al-Skeini,* §§ 133-137.
[29] *Lopez Burgos,* § 12.3.
[30] *Drozd i Janousek protiv Francuske i Španjolske*, presuda od 26. lipnja 1992., Serija A br. 240; *Izvještaj,* § 33.
[31] Europski sud za ljudska prava, *Extra-territorial jurisdiction of States Parties to the European Convention on Human Rights*, *Factsheet,* veljača 2016., dostupno na: http://www.echr.coe.int/documents/fs_extra-territorial_jurisdiction_eng.pdf (pristup 3. prosinca 2016.); *Loizidou protiv Turske*, presuda od 23. ožujka 1995. (prethodni prigovori), Serija A br. 310, *Loizidou protiv Turske*, presuda od 18. prosinca 1996. (osnovanost).
[32] Marko Milanović, *Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age*, 56 HARV. INT'L L. REV. 81 (2015), 120 [*Milanović*].
[33] *Izvještaj*, § 34.
[34] Peter Margulies, *The NSA in Global Perspective: Surveillance, Human Rights, and International Counterterrorism*, 82 Ford. L. Rev. 2137 (2014), str. 2150; *Milanović,* str. 129.

Bez ulaženja u analize takve vrste, određeni broj međunarodnih organizacija i tijela, kao što su UN,[35] Vijeće Europe[36] i Europski parlament,[37] stoji na stanovištu da elektronički nadzor (strane) komunikacije sa sobom povlači primjenu instrumenata za zaštitu ljudskih prava. Također, u određenom broju predmeta vođenih pred ESLJP-om i Odborom za ljudska prava tužene države nisu isticale prigovore nenadležnosti suda u predmetima s ekstrateritorijalnim elementom, prešutno dakle prihvaćajući primjenjivost EKLJP-a, odnosno MPGPP-a, i u takvim situacijama.[38]

Može se dakle zaključiti da međunarodnopravni trend pokazuje u pravcu prihvaćanja ekstrateritorijalne primjene međunarodnih instrumenata za zaštitu ljudskih prava, i to u kontekstu masovnog praćenja elektroničkih komunikacija. Međutim stajalište nekih država o tom pitanju i dalje ostaje neizmijenjeno, posebice onih koje u najvećoj mjeri provode tu praksu. Tako je SAD pri izglasavanju Rezolucije Opće skupštine UN-a o pravu na privatnost u digitalno doba ponovio svoju opetovanu poziciju o ekstrateritorijalnoj neprimjenjivosti MPGPP-a.[39]

2.2. Sadržaj prava na privatnost u digitalnom dobu

Digitalno doba u kojem se svijet nalazi, a koje se očituje u takoreći preseljenju našeg života u virtualnu realnost, gdje se napose komunikacija, a potom i ostale životne navike i radnje, sele na digitalne komunikacijske kanale i platforme, povlači za sobom i potrebu redefiniranja pravnih pojmova i odnosa u kontekstu prava na privatnost. Takva promjena životnih navika, izazvana napretkom i dostupnošću visoke tehnologije, prepoznata je i od UN-a, pa je Opća skupština u Rezoluciji o pravu na privatnost u digitalno doba navela kako

[35] UNGA, *The Right to Privacy in the Digital Age*, UN Doc. A/C.3/68/L.45/Rev.1, 20. studenog 2013.; UNGA, *Resolution on the Right to Privacy in the Digital Age*, UN Doc. A/RES/68/167 od 21. siječnja 2014. [*Rezolucija*]. Radi se o rezoluciji koji su kao reakciju na otkrića Edwarda Snowdena u UN-u inicirale Njemačka i Brazil, a koja je bila prihvaćena bez glasovanja. Rezolucijom je pozvan i Odbor za prava čovjeka da sastavi izvještaj o zaštiti i promociji prava na privatnost u kontekstu domaćeg i ekstrateritorijalnog masovnog praćenja. Odbor je 30. lipnja 2014. izdao *Izvještaj Ureda Visokog povjerenika za ljudska prava* (A/HRC/27/37);
Odbor za prava čovjeka, *Concluding observations on the fourth periodic report of the United States of America,* UN Doc. CCPR/C/USA/CO/4 od 23. travnja 2014.; Odbor za prava čovjeka, *Resolution on promotion, protection and enjoyment of human rights on the Internet,* UN Doc. A/HRC/32/L.20 od 1. srpnja 2016.; UNGA, *The Right to Privacy in the Digital Age,* UN Doc. A/C.3/71/L.39/Rev.1, 16. studenoga 2016.

[36] Vijeće Europe, *Rezolucija Parlamentarne skupštine Vijeća Europe od 21. travnja 2015. o masovnom nadzoru* (Rezolucija 2045 (2015)).

[37] Europski parlament, *Izvješće o postojanju globalnog sustava za presretanje privatne i komercijalne komunikacije (Sustav za presretanje ECHELON*) (2001/2098(INI)), 11. srpnja 2001., str 134; Europski parlament, *Rezolucija Europskog parlamenta od 29. listopada 2015. o daljnjem postupanju nakon usvajanja Rezolucije Europskog parlamenta o elektroničkom masovnom nadzoru građana EU-a 12. ožujka 2014*. (2015/2635(RSP)).

[38] *Milanović*, str. 125, bilješka 179, str. 127.

[39] United States Mission to the United Nations, *Explanation of Position for the Third Committee Resolution on the Right To Privacy in the Digital Age by Ambassador Elizabeth Cousens, U.S. Representative to the UN Economic and Social Council,* 26. studenoga 2013., dostupno na: https://usun.state.gov/remarks/5888 (pristup 20. prosinca 2016.); *Milanović;* str. 85, bilj. 17; *Deeks*, str. 307, bilj. 49.

se sva ljudska prava koja su zajamčena *offline* moraju štititi i *online,* a posebice u kontekstu digitalnih komunikacija i masovnog elektroničkog praćenja.[40]

Instrumenti za zaštitu ljudskih prava ne sadrže definiciju prava na privatnost, nego se u uređenju zaštite tog prava zadržavaju na zabrani arbitrarnog i nezakonitog upletanja u privatnost, obiteljski život, dom ili korespondenciju te jamče da svatko ima pravo na pravnu zaštitu protiv takva upletanja. EKLJP šire uređuje mogućnost pravnog ograničenja prava na privatnost, za koje navodi da mora biti potrebno u demokratskom društvu u interesu nacionalne sigurnosti, javnog reda i mira ili gospodarske dobiti te zemlje te radi sprečavanja nereda i zločina, za zaštitu zdravlja i morala ili radi zaštite prava i sloboda drugih. Američka konvencija o pravima čovjeka, osim arbitrarnog upletanja u uživanje prava na privatnost, zabranjuje i njegovo nasilno ometanje (*abusive interference*).[41]

Kako se pravo na privatnost zapravo definira putem zabrane njegova kršenja, mehanizmi za zaštitu ljudskih prava tražili su njegov sadržaj upravo kroz ispitivanja načina i mehanizama za kršenje.[42] ESLJP je tako utvrdio da se sadržaj prava na privatnost odnosi i na komunikaciju e-poštom, videopozivima i internetskim *chatom,*[43] a u određenim slučajevima i na metapodatke. Naime sustavi za masovni nadzor često sakupljaju metapodatke (*metadata*),[44] koji predstavljaju podatke o komunikacijama (npr. podatke o datumu, lokaciju i brojeve, odnosno adrese osoba koje stupaju u kontakt, bez sadržaja same komunikacije),[45] ali ne i sam sadržaj komunikacije. ESLJP je stava da u određenim slučajevima prikupljanje metapodataka samo za sebe ne predstavlja kršenje prava na privatnost s obzirom na to da mjerenje tih podataka nije isto što i presretanje sadržaja tih podataka,[46] ali da daljnje dijeljenje i prosljeđivanje tih podataka može predstavljati kršenje prava na privatnost zajamčenog člankom 8. EKLJP-a.[47] Sličnog je stajališta i

[40] *Rezolucija.*
[41] Organizacija američkih država, *Američka konvencija o pravima čovjeka, "Pakt iz San Josea", Kostarika*, od 22. studenog 1969., 1144 UNTS 123.
[42] Ujedinjeni narodi, Posebni izvjestitelj za promicanje i zaštitu ljudskih prava i temeljnih sloboda u borbi protiv terorizma, *Četvrto godišnje izvješće podneseno Općoj skupštini*, UN Doc. A/69/397 od 23. rujna 2014.: "Prava je istina da uporaba tehnologije za masovni nadzor učinkovito i u potpunosti uklanja pravo na privatnost komunikacije na internetu."
[43] *Milanović*, str 134; *Kennedy protiv Ujedinjenog Kraljevstva* (presuda), br. 26839/05, ESLJP (2010) [*Kennedy]*; *Liberty i drugi protiv Ujedinjenog Kraljevstva* (presuda), br. No. 58243/00, ESLJP (2008) [*Liberty*].
[44] The Washington Post, *How the NSA's MUSCULAR program collects too much data from Yahoo and Google*, dostupno na: http://apps.washingtonpost.com/g/page/world/how-the-nsas-muscular-program-collects-too-much-data-from-yahoo-and-google/543/ (pristup 20. prosinca 2016.); *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism* (*USA PATRIOT ACT*) *Act of* 2001, od 26. listopada 2001., Section 215: *Access to records and other items under the Foreign Intelligence Surveillance Act*, dostupno na: https://www.gpo.gov/fdsys/pkg/BILLS-107hr3162enr/pdf/BILLS-107hr3162enr.pdf (pristup 20. prosinca 2016.).
[45] *Malone protiv Ujedinjenog Kraljevstva* od 2. kolovoza 1984., serija A br. 82, [*Malone*] § 56; *Escher protiv Kolumbije*, presuda od 6. srpnja 2009., IASLJP (ser. C), br. 200 [*Escher*], § 114.
[46] *Malone*, § 84; *P. G. i J. H. protiv Ujedinjenog Kraljevstva* (presuda), br. 44787/98, ESLJP (2001), § 42.
[47] *Malone*, §§ 86-88.

Interamerički sud za ljudska prava, koji je utvrdio da su metapodaci, jednako kao i sadržaj komunikacije, zaštićeni aspekti prava na privatnost.[48]

U tom je smislu bitno naglasiti da pohrana podataka i daljnje dijeljenje podataka prikupljenih tajnim nadzorom s trećom stranom mogu predstavljati zasebnu daljnju povredu prava na privatnost.[49]

U kontekstu sustava za masovni nadzor ESLJP je pak naglasio kako i sama činjenica postojanja zakonodavnog okvira koji omogućuje tajni nadzor komunikacija povlači za sobom prijetnju koja predstavlja udarac na slobodu komunikacije korisnika telekomunikacijskih usluga te na taj način sama po sebi predstavlja upletanje u pravo na privatnost, bez obzira na postojanje stvarnih mjera koje su poduzete protiv pojedinca.[50] Da samo postojanje sustava za masovno praćenje predstavlja upletanje u pravo na privatnost, potvrdio je i Odbor za prava čovjeka.[51]

2.3. Ograničenja prava na privatnost u digitalnom dobu

Kada je u pitanju sraz ljudskih prava i zaštite nacionalne sigurnosti, doba u kojem živimo naziva se i *Post 9/11 era*, a označava razdoblje nakon napada na zgrade Svjetskog trgovinskog centra u New Yorku 11. rujna 2001. godine, ali i druge terorističke napade (napadi u Madridu 2004. godine i Londonu 2005. godine). Međunarodni odgovori na te napade, osim onih silom, sadržavali su i robusnu legislativnu djelatnost od strane međunarodnih organizacija: UN-a[52] i EU-a,[53] kao i država koje su bile izravno pogođene napadima.[54] Svi ti odgovori pod zajedničkim su nazivnikom borbe protiv terorizma, odnosno zaštite nacionalne sigurnosti, nauštrb uživanja ljudskih prava, posebice prava na

---

[48] *Escher,* § 114.
[49] *Weber,* § 79.
[50] *Milanović,* str. 134; *Weber,* § 78; *Malone*, § 64.
[51] *Izvještaj,* § 20.
[52] Vijeće sigurnosti, *Resolution 1373 (2001),* UN Doc. S/RES/1373 (2001) od 28. rujna 2001., Vijeće sigurnosti, *Report of the Policy Working Group on the United Nations and Terrorism*, UN Doc. A/57/273-S/2002/875; Report of the Secretary-General, Commission on Crime Prevention and Criminal Justice, *Strengthening international cooperation and technical assistance in promoting the implementation of the universal conventions and protocols related to terrorism within the framework of the activities of the United Nations Office on Drugs and Crime*, UN Doc. E/CN.15/2005/ od 13. svibnja 2005.
[53] *Direktiva 2006/24/EZ Europskog parlamenta i Vijeća od 15. ožujka 2006. o zadržavanju podataka dobivenih ili obrađenih u vezi s pružanjem javno dostupnih elektroničkih komunikacijskih usluga ili javnih komunikacijskih mreža i o izmjeni Direktive 2002/58/EZ* (SL L 105, str. 54) (SL, posebno izdanje na hrvatskom jeziku, poglavlje 13, svezak 50, str. 30); vidi i *Presuda Suda (veliko vijeće) od 8. travnja 2014. (zahtjev za prethodnu odluku koji su uputili High Court of Ireland, Verfassungsgerichtshof – Irska, Austrija) – Digital Rights Ireland Ltd (C-293/12), Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl i dr. (C-594/12) protiv Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, The Commissioner of the Garda Síochána, Ireland and the Attorney General* (Spojeni predmeti C-293/12 i C-594/12).
[54] Stephen P. Marks, *International Law and the 'War on Terrorism': Post 9/11 Responses by the United States and Asia Pacific Countries,* 14 Asia Pacific Law Review 43 (2006). Određeni autori ističu kako je nakon napada 11. rujna 2011. godine pao „zid" između dopustivosti korištenja obavještajnih podataka za potrebe nacionalne sigurnosti i ostale potrebe, a što se ogleda u slabljenju zaštite osobnih podataka, odnosno privatnosti, *Ira Rubenstein i dr*., str. 114.

privatnost.[55] Upravo su pozivanjem na potrebu zaštite nacionalne sigurnosti opravdavani sustavi za masovni elektronički nadzor komunikacija.[56] I dok se državama ne može ograničavati pravo na izbor sredstva za osiguranje nacionalne sigurnosti[57] (jer je prije svega riječ o *domaine reserve)*[58] te im se u tom smislu osigurava određeno diskrecijsko pravo *(margin of appreciation),*[59] predmetni izbori država ipak mogu biti podložni ispitivanju od strane mehanizama za zaštitu ljudskih prava. Kao što je već naznačeno, Odbor za prava čovjeka i ESLJP povukli su široki zaključak da sustavi za masovno praćenje *per se* predstavljaju ograničenje prava na privatnost. Međutim upletanje u pravo na privatnost ne predstavlja samo po sebi kršenje tog prava. Naime pravo na privatnost nije apsolutno jer su, pod određenim uvjetima, upletanja od strane državnih vlasti dopuštena.

Na ovom je mjestu potrebno upozoriti na određene razlike koje u vezi s ograničenjem uživanja prava na privatnost postoje s obzirom na derogiranje uživanja prava zajamčenih instrumentima za zaštitu ljudskih prava temeljem derogacijske klauzule. Naime instrumenti za zaštitu ljudskih prava sadrže derogacijsku klauzulu,[60] koja omogućuje državama derogiranje obveze poštovanja prava koja su zajamčena predmetnim instrumentom. Derogacija mora biti vremenski privremena, sadržajno ograničena te mora poštovati propisani postupak notifikacije. Derogacijsku klauzulu moguće je koristiti samo u ratu i izvanrednim stanjima koja ugrožavaju opstanak naroda, a ona omogućuje ograničenje uživanja ljudskih prava, uz iznimku određenih prava (ovisno o instrumentu).[61] Posljednji primjeri korištenja derogacijske klauzule s obzirom na EKLJP jesu derogacija Francuske Republike od 24. studenog 2015. godine.[62] Klauzula je bila podignuta u kontekstu odgovora na jezive terorističke napade na Pariz 13. studenog 2015. godine. Francuska je aktivacijom i produljivanjem primjene Zakona o izvanrednom stanju (*Loi n° 55-385 du 3 avril 1955 relative à l'état d'urgence*) derogirala obveze koje proistječu iz EKLJP-a kao odgovor na „terorističku prijetnju koja predstavlja neposrednu opasnost

[55] Odbor za prava čovjeka, *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism,* UN Doc. E/CN4/2006/98*,* 28. prosinca 2005.
[56] *Govor predsjednika Obame*; The Guardian, *UK spy agencies need more powers, says Cameron,* 12. siječnja 2015., videozapis govora dostupan je na: https://www.theguardian.com/uk-news/2015/jan/12/uk-spy-agencies-need-more-powers-says-cameron-paris-attacks (pristup 20. prosinca 2016.)*; Izvještaj*, § 23.
[57] *Szabó i Vissy protiv Mađarske* (presuda), broj 37138/14, ESLJP (2016), [*Szabó*] § 73, 178.
[58] Povelja, čl. 2., § 7.
[59] *Szabó,* § 57.
[60] EKLJP, čl. 15.; MPGPP, čl. 4.
[61] EKLJP tako zabranjuje derogaciju prava na život, osim u okolnostima zakonitih radnja u ratu; zabrane mučenja i nečovječnog postupanja ili kazne; zabrane ropstva te pravila „nema kazne bez zakona"; zabrane smrtne kazne u miru i u svim okolnostima te pravila da se nikom ne može suditi dva puta u istoj stvari. Slično, MPGPP zabranjuje derogaciju prava na život, prava na slobodu od mučenja i nečovječnog postupanja ili kazne te podvrgavanja medicinskom ili znanstvenom istraživanju; zabrane ropstva ili odnosa sličnog ropstvu; te načela *ne bis in idem*.
[62] Vijeće Europe, *France informs Secretary General of Article 15 Derogation of the European Convention on Human Rights*, 25. studenog 2015., dostupno na: https://www.coe.int/en/web/secretary-general/news/-/asset_publisher/EYlBJNjXtA5U/content/france-informs-secretary-general-of-article-15-derogation-of-the-european-convention-on-human-rights (pristup 20. prosinca 2016. godine).

koja proizlazi iz ozbiljnih kršenja javnog reda te opravdava inicijalnu derogaciju izvanrednog stanja i njezino produljenje."[63]

Pravo na privatnost može biti obuhvaćeno i derogacijskom klauzulom. Međutim iz samih odredaba koje uređuju pravo na privatnost proizlazi da je njegovo ograničavanje moguće i izvan stanja izvanrednih okolnosti. Ograničavanje mora zadovoljavati zahtjeve zakonitosti i zabrane samovolje od strane države.[64] U nastavku rada razrađujemo uvjete koji moraju biti zadovoljeni da bi opravdali ograničenje uživanja prava na privatnost.

2.3.1. Ograničenje je u skladu sa zakonom

Kao što proizlazi iz teksta relevantnih instrumenata, svako ograničenje prava na privatnost mora biti utemeljeno na zakonu.[65] Djelovanje mehanizama za zaštitu prava čovjeka dalje je razradilo ovaj uvjet, i to u kontekstu sustava za nadzor, te se praksom navedenih tijela iskristaliziralo nekoliko zahtjeva koje domaći pravni okviri za ograničavanje uživanja prava na privatnost moraju zadovoljavati.[66] Iako programi za masovni nadzor mogu biti (i u najvećem broju slučajeva jesu) utemeljeni na domaćem zakonodavstvu, njihovo neslaganje s međunarodnim instrumentima za zaštitu prava čovjeka može ih učiniti nezakonitima u „očima" tih zahtjeva, odnosno međunarodnog prava.[67] Istovremeno, kršenje zahtjeva postavljenih domaćim pravnim okvirom automatski čini ograničenje prava nezakonitim na taj način kršeći međunarodno pravo.[68]

Zahtjevi za legalnost ograničenja prava na privatnost u kontekstu tajnog nadzora elektroničkih komunikacija mogu se sumirati kao sljedeći. Zakonski okvir koji omogućuje nadzor mora biti javno dostupan,[69] jasan i precizan[70] na način da svaki zainteresirani pojedinac može konzultirati zakonski okvir i utvrditi tko je u kojim okolnostima[71] i na koji način (postupak)[72] ovlašten poduzeti nadzor.[73] Preciznost zakonodavnog okvira očituje se i u specifikaciji kategorija osoba koje mogu biti stavljanje pod nadzor,[74] kao i duljine

[63] *Id.*
[64] *Donoso protiv Paname,* presuda od 27. siječnja 2009., IASLJP (ser. C) br. 193.
[65] UN Commission on Human Rights, *Siracusa Principles on the Limitation and Derogation of Provisions in the ICCPR*, UN Doc. E/CN.4/1984/4, od 29. rujna 1984.
[66] *Izvještaj*, §§ 21-30.
[67] *Id.*, § 21.
[68] *Milanović*, str. 135; *Klass i drugi protiv Njemačke,* 6. rujna 1978., serija A br. 28, [*Klass*], § 43; *Weber*, § 90.
[69] *Liberty,* §§ 60-61, 63; *Shimovolos protiv Rusije* (presuda), br. 30194/09, ESLJP (2011), § 67 i dalje.
[70] *Escher,* § 130.
[71] *Klass*, §§ 43, 46, 96; *Weber*, § 85.
[72] *Escher*, § 131; *Klass*, § 51; *Weber*, § 115.
[73] *Izvještaj*, § 23; *Malone*, § 67; Odbor za prava čovjeka, *Komentar broj 903/1999 (Van Hulst protiv Nizozemske),* UN Doc. CCPR/C/82/D/903/1999 od 15. studenog 2004., § 7.7.
[74] *Escher*, § 131.

nadzora[75] te daljnjeg čuvanja i raspolaganja sakupljenim podacima.[76] Navedeno je oblikovano kao *zahtjev predvidljivosti* (*foreseeability*).[77]

Oživotvorenje navedenih kriterija možemo promatrati na primjeru zakonodavnog okvira koji u Ujedinjenom Kraljevstvu uređuje, među ostalim, nadzor i presretanje komunikacija. Naime ESLJP je u dva navrata ispitivao navedeni zakonodavni okvir. U predmetu iz 2008. godine *Liberty i drugi protiv Ujedinjenog Kraljevstva* sud je ispitivao *The Interception of Communications Act 1985* u kontekstu povrede prava na privatnost te utvrdio kako predmetni zakon nije precizno uredio obujam i način na koji država izvršava upletanje u uživanje prava na privatnost, pri čemu ima široko diskrecijsko pravo. Navedeno je potrebno kako bi se osigurala primjerena zaštita protiv zlouporaba ovlasti. Sud je posebno naglasio kako zakonski akt nije izložio u formi dostupnoj javnosti ni natruhe postupka za pregled, dijeljenje, pohranjivanje i uništavanje presretnutog materijala. Iz tih je razloga sud utvrdio da upletanje u pravo na privatnost nije u skladu člankom 8. Konvencije.[78]

U drugom navratu ESLJP je u predmetu *Kennedy protiv Ujedinjenog Kraljevstva* ispitivao zakonski akt *RIPA 2000*,[79] donesen kako bi zamijenio *The Interception of Communications Act 1985* te na odgovarajući način zaštitio uživanje ljudskih prava u okolnostima napretka tehnologije.[80] Tada je Sud ispitivao navode podnositelja zahtjeva kako ni *RIPA 2000*, kao zakonodavni akt koji je stavio izvan snage *The Interception of Communications Act 1985*, ne zadovoljava zahtjeve koje je pred britanskog zakonodavca stavio ESLJP u predmetu.[81]

Međutim sud nije udovoljio zahtjevu podnositelja te je utvrdio kako *RIPA 2000* zadovoljava zahtjev predvidljivosti te se stoga ograničenja prava privatnosti koja akt omogućuje mogu smatrati zakonitima. Sud je u prilog svojeg zaključka naveo sljedeće karakteristike *RIPA 2000*:

- akt je javno dostupan dokument objavljen na internetu[82]
- iako akt ne navodi izrijekom kaznena djela za koja je moguće provesti nadzor, navodi prirodu tih djela[83]

---

[75] *Klass*, § 52; *Weber*, § 98.
[76] *Kruslin protiv Francuske* i *Huvig protiv Francuske*, 24. travnja 1990., serija A nos 176 A i 176 B, §. 34; *Amann protiv Švicarske* (presuda) br. 27798/95, ESLJP (2000-II), § 76.
[77] Sud je posebno naglasio kako „predvidljivost u posebnom kontekstu tajnih obavještajnih mjera ne može značiti da pojedincu treba biti omogućeno predvidjeti kada će vlasti presretati njegovu komunikaciju kako bi se on mogao prilagoditi toj činjenici (*Malone*, § 67); *Rotaru protiv Rumunjske* (presuda), br. 28341/95, ESLJP 2001. [*Rotaru*], § 52.
[78] *Liberty,* § 69.
[79] *RIPA 2000*, *Introductory Text*.
[80] *RIPA 2000, Explanatory note,* čl. 8.
[81] *Kennedy*, §§ 135, 150: Podnositelj zahtjeva nije osporavao činjenicu da sustav nadzora koji omogućuje *RIPA 2000* ima za legitiman cilj zaštitu nacionalne sigurnosti, prevenciju zločina i gospodarsku dobrobit zemlje.
[82] *Kennedy*, § 157.
[83] *Id.,* § 159.

- akt ne dopušta nasumično (*indiscrimninate)* masovno presretanje,[84] pa je u tom kontekstu prihvatljivo što akt ne navodi kategorije osoba nad kojima je moguće provoditi nadzor, a posebice jer se radi o presretanju domaćih komunikacija unutar Ujedinjenog Kraljevstva[85]
- akt jasno propisuje maksimalno vrijeme trajanja naloga koji omogućuje praćenje i uvjete za njegovo produljenje (iako se nalog može neograničeno produljiti)[86]
- akt ograničava diskrecijsko pravo nadležnih vlasti u presretanju komunikacije na način da ga omogućuje samo s obzirom na određenu osobu i određeni set okolnosti, a prikupljeni podaci mogu biti dostupni samo određenom krugu osoba s odgovarajućom sigurnosnom provjerom,[87] dok se prikupljeni podaci koji nisu nužni za svrhu presretanja moraju uništiti[88]
- akt je uspostavio tijelo ovlašteno za nadzor djelovanja sustava nadzora i presretanja komunikacija uspostavljenog samim aktom,[89] koji je neovisan o izvršnoj i zakonodavnoj vlasti, a radi se o osobi koja drži ili je držala visoku sudačku poziciju, te izvješće o funkcioniranju sustava za nadzor predaje premijeru.[90]

Sva ta svojstva zakonodavnog okvira (*RIPA 2000*) sud je smatrao dovoljnim jamstvima protiv zloporabe ograničenja prava na privatnost te u skladu s člankom 8. stavkom 2. EKLJP-a.

2.3.2. Ograničenje je nužno i proporcionalno legitimnom cilju

Zahtjevi nužnosti i proporcionalnosti svojevrsni su međunarodnopravni standardi primjenjivi pri poduzimanju međunarodnopravnih radnja s posljedicama po druge međunarodne subjekte ili s obzirom na pojedince.[91] U kontekstu ograničenja prava na privatnost ta dva načela očituju se u zahtjevu da ograničenje prava mora biti minimalno, odnosno u onoj mjeri koja nema za učinak njegovo potpuno onemogućivanje,[92] a na način da se za ograničavanje prava koristi najmanje intruzivno sredstvo.[93]

Da bi se utvrdilo krši li određena mjera pravo na privatnost, potrebno je provesti ispitivanje ravnoteže mjere i legitimnog cilja, odnosno potrebno je preispitati nužnost i prirodu mjere (kojom se namjerava postići legitiman cilj) s obzirom na ozbiljnost

[84] *Id.,* § 160.
[85] *Id.*
[86] *Id.,* § 161.
[87] *Id.,* § 163.
[88] *Id.,* § 162.
[89] *Id.,* § 166.
[90] *Id.*
[91] *Id.,* §§ 135, 136.
[92] *Izvještaj,* § 25, bilj. 16.
[93] *Id.,* §§ 23, 25, 27.

upletanja u pravo na privatnost.[94] Samo upletanje ne smije osujetiti bit samog prava te ono ne smije postati pravilo, nego ostati iznimka; ta ravnoteža ne smije se poremetiti.[95]

Kod masovnog nadzora podataka upozorava se na *a priori* nepoštovanje načela proporcionalnosti i nužnosti s obzirom na to da se radi o nadzoru i sakupljanju *en masse,* koji zatiru svaki obzir prema navedenim načelima, omogućujući državi da nadzire i pohranjuje svaki akt komunikacije bez dobivanja odobrenja za pojedini slučaj nadzora.[96] Ta metoda obavještajne djelatnosti može se usporediti s traženjem igle (relevantne informacije) u plastu sijena (kibernetskom prostoru u kojem se virtualna komunikacija odvija), pri čemu nije izvjesno da igla postoji i da se nalazi u plastu. Mjere koje se pri tome poduzimaju, umjesto da ciljaju iglu, obuhvaćaju cijeli plast.[97] Kako bi makar nominalno bile u skladu s načelom proporcionalnosti, države pribjegavaju svojevrsnoj *a posteriori* primjeni načela, koja se ogleda u nametanju ograničenja pristupa tako sakupljenim podacima (umjesto ograničenja pri samom prikupljanju podataka),[98] bilo u obliku ograničenja osoba koje im mogu pristupati bilo u obliku metode analize tih podataka.[99]

Legitiman cilj treći je kumulativni element tog zahtjeva. ESLJP je dao tumačenje da Konvencija može „tolerirati" tajni nadzor u onoj mjeri u kojoj je on nužan za očuvanje demokratskih institucija.[100] Također, sud je naglasio kako države imaju određeno diskrecijsko pravo pri određivanju jesu li upletanja „potrebna u demokratskom društvu" u ostvarivanju legitimnog cilja zaštite nacionalne sigurnosti, kao i u ocjeni proporcionalnosti upletanja u uživanje prava.[101] U predmetu *Weber* ESLJP je tako odbio zahtjev podnositelja koji je tvrdio da strateško nadziranje u obliku snimanja telekomunikacija, kao i korištenje osobnih podataka te njihovo daljnje dijeljenje, predstavlja kršenje članka 8. EKLJP-a, s argumentom da njemački zakonodavni okvir pruža primjerena i učinkovita jamstva protiv zloporabe predmetnog sustava za nadzor, a da je upletanje u tajnost komunikacija potrebno u demokratskom društvu u interesu zaštite nacionalne sigurnosti i sprečavanja kaznenih djela.[102]

---

[94] *Leander protiv Švedske,* 26. ožujka 1987., serija A br. 116 [*Leander*], § 57.
[95] Odbor za prava čovjeka, *General Comment No. 27: Article 12 (Freedom of Movement),* UN Doc. CCPR/C/21/Rev.1./Add. 9 od 2. studenog 1999., §§ 11-16; *Klass*, § 42.
[96] Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression,* UN Doc. A/HRC/23/40 od 17. travnja 2013., § 62; „Takav masovni, neselektivni nadzor inherentno je nerazmjeran i predstavlja neopravdano miješanje u prava zajamčena člancima 7. i 8. Povelje." (CJEU, C-362/14, *Maximillian Schrems protiv povjerenika za zaštitu podataka*, Mišljenje nezavisnog odvjetnika, 23. rujna 2015.)
[97] *Izvještaj,* § 25.
[98] *Id.,* § 27.
[99] Foreign Intelligence Surveillance Court, AMENDED MEMORANDUM OPINION, Docket Number: BR 13-109 od 29. kolovoza 2013., str. 5.
[100] *Rotaru*, § 47.
[101] *Kennedy*, § 166.
[102] *Weber i Saravia protiv Njemačke* (odluka), br. 54934/00 ESLJP (2006), [*Weber*]§ 80.

2.3.3. Postojanje pravnih jamstava i odgovarajuće pravne zaštite od ograničenja prava na privatnost

Zahtjev pravnih jamstava i pravne zaštite od upletanja u uživanje prava na privatnost sadržan je u samim odredbama instrumenata za zaštitu ljudskih prava koje se odnose na pravo na privatnost.[103] EKLJP jamči pravo na djelotvoran pravni lijek u zasebnoj odredbi, koja je primjenjiva na sva prava i slobode priznate Konvencijom, pa se stoga ono tretira kao zasebno pravo, odnosno moguća zasebna povreda Konvencije.[104]

Posebnost obavještajnog nadzora jest to što je on u pravilu tajan. Štoviše, njegova učinkovitost i uspješnost ovisi o razini njegove tajnosti. Čak i u novonastalim okolnostima, u kojima je globalnoj javnosti sve jasnije da se vlade država koriste masovnim nadzorom svojih (ali i stranih) građana, pojedinac ne može sa sigurnošću znati da je upravo on meta nadzora. U ranijim je odlukama Europska komisija za ljudska prava bila utvrdila kako postojanje sustava nadzora može utjecati na pravo na privatnost, ali da tvrdnja, odnosno zahtjev za utvrđivanjem kršenja prava na privatnost, može biti opravdana samo kada postoji razumna vjerojatnost *(reasonable likelihood*)[105] da je osoba zaista subjekt nezakonitog nadzora. Taj je standard bio ustanovljen pri odlučivanju o dopustivosti zahtjeva s obzirom na to da se Komisija, odnosno ESLJP, ne upušta u odlučivanje *in abstracto.*[106] Međutim nakon presude u predmetu *Klass* praksa ESLJP-a kretala se na dva paralelna kolosijeka u tumačenju standarda razumne vjerojatnosti,[107] a 2010. godine u predmetu *Kennedy* ESLJP je preuzeo drugi standard te je utvrdio kako pristup sudu treba biti omogućen svim osobama koje su „potencijalno pogođene" mjerama tajnog nadzora.[108] Nedavno je u predmetu *Zakharov* ESLJP, „imajući na umu specifične karakteristike mjera za tajni nadzor te važnosti osiguranja učinkovite kontrole i nadzora nad istima",[109] zauzeo stajalište kako pojedincu treba dopustiti pristup sudu kada tvrdi da je žrtva kršenja prava zajamčenog člankom 8. Konvencije temeljem samog postojanja mjera za tajni nadzor pod dva uvjeta.[110] Prvi uzima u obzir opseg zakonodavnog okvira koji omogućuje tajni nadzor te propituje može li predmetni pojedinac istim biti obuhvaćen na temelju same činjenice da pripada grupi pojedinaca koji su „meta" takva zakonodavnog okvira ili se radi o tome da su pogođeni svi korisnici određenog komunikacijskog servisa. Drugi uvjet uzima u obzir dostupnost djelotvorne zaštite (*effective remedies*) na nacionalnoj razini, pri čemu potpuni izostanak iste može osigurati pristup sudu pojedincu čak i onda kada je mogućnost da je on sam meta tajnog nadzora niska. U tom slučaju pojedinac i ne treba

---

[103] *Opća deklaracija o ljudskim pravima,* čl. 12.; MPGPP, čl. 17., § 2; *Američka konvencija o pravima čovjeka,* čl. 11., § 3; *Arapska povelja o ljudskim pravima,* čl. 21., § 2.

[104] Čl. 13. EKLJP-a, Pravo na djelotvorni pravni lijek: „Svatko čija su prava i slobode koje su priznate u ovoj Konvenciji povrijeđeni ima pravo na djelotvorna pravna sredstva pred domaćim državnim tijelom, čak i u slučaju kad su povredu počinile osobe koje su djelovale u službenom svojstvu."

[105] *Esbester protiv Ujedinjenog Kraljevstva*, zahtjev br. 18601/91 (1993).

[106] *Klass*, § 33; *N.C. protiv Italije* (presuda), broj 24952/94 ESLJP (2002-X), § 56; *Krone Verlag GmbH & Co. KG protiv Austrije* (br. 4), broj 72331/01 ESLJP (2002-X), § 26.

[107] *Zakharov,* str. 39, §§ 166-168.

[108] *Kennedy*, § 120, citira § 35 presude *Klass.*

[109] *Zakharov,* str. 38, § 165.

[110] *Id.,* str. 41, § 171.

dokazivati postojanje rizika da je meta tajnog nadzora. S druge strane, kada dostupna učinkovita zaštita na nacionalnoj razini postoji, u obzir se uzima vjerojatnost da se mjere tajnog nadzora poduzimaju protiv predmetnog pojedinca podnositelja zahtjeva.[111] Dakle razvidno je da je ESLJP tokom godina „olabavio" uvjete pristupanja sudu kada se radi o zahtjevima za utvrđenje povrede prava u kontekstu tajnih nadzora.

Kako proizlazi iz odredaba instrumenata za zaštitu ljudskih prava koje uređuju pravo na privatnost, učinkovit pravni lijek ne mora nužno biti u obliku sudskog postupka. Djelotvoran pravni lijek mogu pružiti kako sudska tako i upravna te izvršna domaća nadležna tijela.[112] U tom smislu, posebno vezano uz učinkovit pravni lijek u slučaju tajnog nadzora, ESLJP je naglasio kako nepristrano nadzorno tijelo može biti dostatno u kontekstu pružanja djelotvornog pravnog lijeka sve dok su mjere tajne. Tek kada se mjere razotkriju pravna sredstva moraju biti dostupna pojedincu.[113]

3. POSEBNO O SIGURNOSNO-OBAVJEŠTAJNOM SUSTAVU U REPUBLICI HRVATSKOJ I USKLAĐENOSTI ZAKONSKOG OKVIRA SA ZAHTJEVIMA ESLJP-A

Republika je Hrvatska država stranka Europske konvencije o ljudskim pravima, čiji je mehanizam za zaštitu i utvrđivanje povrede Konvencije u odnosu na države stranke ESLJP-a. Hrvatski zakonski okvir za obavljanje tajnog nadzora elektroničkih komunikacija nije do sada bio predmetom ispitivanja od strane ESLJP-a,[114] stoga ćemo u sljedećim odlomcima pokušati dati analizu hrvatskog zakonskog okvira u svjetlu zahtjeva za legalnost ograničenja prava na privatnost koje je u relevantnim presudama postavio ESLJP.

3.1. Zakonski okvir obavještajnog djelovanja u Republici Hrvatskoj

Opći zakonski okvir obavještajnog djelovanja u Republici Hrvatskoj zadan je Zakonom o sigurnosno-obavještajnom sustavu Republike Hrvatske.[115] Njime su osnovane sigurnosno-obavještajne agencije:[116] Sigurnosno-obavještajna agencija [SOA] i Vojna sigurnosno-obavještajna agencija [VSOA].

Opći zakonski okvir određuje da SOA može prema građanima primjenjivati mjere tajnog prikupljanja podataka kojima se privremeno ograničavaju neka ustavna ljudska prava i temeljne slobode ako se podaci ne mogu prikupiti na drugi način. Mjere tajnog prikupljanja podataka kod tajnog nadzora telekomunikacijskih usluga, djelatnosti i

111 *Id.*
112 *Izvještaj,* § 13.
113 *Segerstedt-Wiberg i drugi protiv Švedske* (presuda), broj 62332/00 ESLJP (2006), § 117.
114 Predmeti *Dragojević protiv Hrvatske* (zahtjev broj 68955/11) i *Bašić protiv Hrvatske* (zahtjev broj 22251/13), u kojima je ESLJP utvrdio postojanje povrede članka 8. EKLJP-a, ticali su se ograničenja prava na privatnost u kontekstu kaznenog postupka, a ne u obavještajnom kontekstu.
115 Zakon o sigurnosno-obavještajnom sustavu Republike Hrvatske [ZSOS] (NN 79/06, 105/06).
116 *Id.,* čl. 1.

prometa jesu: a) tajni nadzor sadržaja komunikacija, b) tajni nadzor podataka o telekomunikacijskom prometu, c) tajni nadzor lokacije korisnika, d) tajni nadzor međunarodnih telekomunikacijskih veza.[117]

Posebni zakonski okvir s obzirom na nadzor elektroničkih komunikacija čine odgovarajući komplementarni zakonski i podzakonski akti: Zakon o elektroničkim komunikacijama[118] i Uredba o obvezama iz područja nacionalne sigurnosti Republike Hrvatske za pravne i fizičke osobe u telekomunikacijama,[119] koji dalje razrađuju odredbe članaka 18., 19. i 33. ZSOS-a, koji se odnose na mjere tajnog prikupljanja podataka.

Svi navedeni akti javno su objavljeni i dostupni javnosti, odnosno zainteresiranom pojedincu. Osnovni je to element zahtjeva predvidljivosti koji ESLJP postavlja.[120] U njima je također navedeno u kojim se okolnostima može obavljati tajni nadzor komunikacija (ako se podaci ne mogu prikupiti na drugi način), iz čega proizlazi da je tajni nadzor komunikacija posljednje sredstvo kojemu treba pribjegavati u obavljanju obavještajne djelatnosti. Time se već u samoj zakonskoj odredbi nameće poštivanje načela proporcionalnosti, načela koje je ključno u ocjeni zakonitosti ograničenja prava na privatnost.[121] U tom smislu bitna je i odredba članka 36. stavka 4. ZSOS-a, iz koje jasno proizlazi da se mjera tajnog praćenja može poduzeti samo prema pojedinoj fizičkoj ili pravnoj osobi, što ide u prilog poštovanju načela proporcionalnosti, s obzirom na to da se takav tajni nadzor ne obavlja ni arbitrarno ni nasumično.[122]

3.1.1. Postupak određivanja mjera tajnog praćenja

Vezano uz sam postupak određivanja mjera tajnog praćenja, ZSOS sadrži niz odredaba kojima se postupak uređuje, počevši od zahtjeva pisanog obrazloženja prijedloga za nalaganje mjera tajnog praćenja, koji podnosi ravnatelj SOA-e ili VSOA-e. Sam nalog izdaje ovlašteni sudac Vrhovnog suda u formi pisanog obrazloženog naloga, a nalog (kao i prijedlog) mora sadržavati oznaku mjere koja će se primjenjivati, oznaku fizičke ili pravne osobe prema kojoj će se mjera primjenjivati, obrazloženje razloga zbog kojih se mjera provodi i potrebe njezina poduzimanja i rok trajanja mjere. Ako se predlaže i dopušta poduzimanje više mjera, moraju biti navedeni podaci za svaku mjeru.[123] Iz navedenog proizlazi da je za nalaganje mjera za tajno praćenje nadležna sudska, a ne izvršna vlast.

---

[117] ZSOS, čl. 33.
[118] Zakon o elektroničkim komunikacijama (NN 73/08, 90/11, 133/12, 80/13, 71/14), čl. 108.: *Tajni nadzor elektroničkih komunikacijskih mreža i usluga*, čl. 109.: *Obveza zadržavanja podataka*, čl. 110.: *Vrste zadržanih podataka.*
[119] Uredba o obvezama iz područja nacionalne sigurnosti Republike Hrvatske za pravne i fizičke osobe u telekomunikacijama (NN 64/2008).
[120] *Liberty*, §§ 60-61, 63; *Shimovolos protiv Rusije* (presuda), br. 30194/09, ESLJP 2011, §§ 67 i dalje.
[121] Vidi *supra* 2.3. iii.
[122] *Kennedy*, § 160, *Szabó*, §§ 66, 67.
[123] *Id.,* čl. 36., § 4.

Stavljanje odobravanja mjera tajnog praćenja isključivo u ruke izvršne vlasti kao jedan od elemenata kršenja članka 8. EKLJP-a naveo je ESLJP u presudi u predmetu *Szabó.*[124]

Nadalje, člankom 37. ZSOS-a uređeno je maksimalno trajanje mjera (4 mjeseca), kao i postupak za eventualno produljenje ili primjenu novih mjera nad istom osobom. U tom slučaju zakon nalaže stroži postupak odobravanja, u kojem sudjeluje vijeće od tri ovlaštena suca Vrhovnog suda, koje je ovlašteno zatražiti dodatna mišljenja i obrazloženja ne samo od predlagatelja nego i od Vijeća za nacionalnu sigurnost (stavak 3.).[125] Vezano uz samo postupanje sa sakupljenim podacima, ZSOS sadrži niz odredaba koje jamče da podacima rukuju djelatnici agencija koji imaju odgovarajući stupanj sigurnosne provjere te koji su dužni saznanja o primjeni mjera tajnog prikupljanja podataka čuvati kao tajnu.[126] Nadalje, dokumenti o podacima koji se ne odnose na svrhu radi koje su prikupljani, kao i podaci, dokumenti i informacije koji su prikupljeni na nezakonit način, uništavaju se u roku od 30 dana.[127] Navedene odlike postupanja s podacima prikupljenima tajnim nadzorom u skladu su s traženjima ESLJP-a u predmetu *Kennedy*.[128]

3.1.2. Pravna jamstva i nadzor nad ograničavanjem prava na privatnost

ZSOS također sadrži velik broj pravnih jamstava i odredaba o pravnoj zaštiti u ograničavanju prava na privatnost prilikom korištenja mjera tajnog nadzora. Tako su sigurnosno-obavještajne agencije dužne na zahtjev građanina u roku od 15 dana obavijestiti ga pisanim putem jesu li prema njemu poduzimane mjere tajnog prikupljanja podataka te vode li se evidencije o njegovim osobnim podacima te na njegov zahtjev staviti mu na uvid dokumente o prikupljenim podacima.[129] U ovome kontekstu potrebno je posebno naglasiti da ESLJP ne traži da država objavi odluku o stavljanju pod mjere u slučaju kada je ta mjera poduzeta unutar zakonitog programa domaćeg nadzora niti traži da država naknadno i posebno obavijesti osobu o činjenici da je se tajno prati.[130] Stoga možemo kazati da to pravno jamstvo koje zakon omogućuje nadilazi obveze koje RH kao država stranka EKLJP-a ima u tom pogledu.

Vezano uz nadzor rada sigurnosno-obavještajnih agencija, članak 103. Zakona propisuje tijela za nadzor, a to je Hrvatski sabor, koji nadzor obavlja neposredno ili putem Ureda Vijeća za nacionalnu sigurnost i Vijeća za građanski nadzor sigurnosno-obavještajnih agencija.[131] Odbor Hrvatskoga sabora nadležan za nacionalnu sigurnost[132] ovlašten je obavljati nadzor nad tijelima sigurnosno-obavještajnog sustava u skladu sa zakonom osobito što se tiče zaštite Ustavom Republike Hrvatske utvrđenih ljudskih prava i

[124] *Szabó*, § 62, 65.
[125] Odgovara zahtjevu koji je postavio ESLJP u predmetu *Kennedy,* § 161.
[126] ZSOS, čl. 35. i čl. 39.*;* odgovara zahtjevu koji je postavio ESLJP u predmetu *Kennedy,* § 162.
[127] ZSOS, čl. 41.*;* odgovara zahtjevu koji je postavio ESLJP u predmetu *Kennedy,* § 163.
[128] *Kennedy*, §§ 161-163.
[129] ZSOS, čl. 40.
[130] *Klass,* § 58.
[131] ZSOS, čl. 104.
[132] Poslovnik Hrvatskoga sabora (NN, 81/13), čl. 69: *Odbor za unutarnju politiku i nacionalnu sigurnost*.

temeljnih sloboda. U provedbi nadzora Odbor može zatražiti, među ostalim, izvješća o provođenju mjera tajnog prikupljanja podataka ili o provođenju mjera tajnog prikupljanja podataka prema određenim osobama.[133] Također, Odbor je ovlašten razmatrati izvješće pučkog pravobranitelja o zaštiti ustavnih i zakonskih prava građana u postupcima koje poduzimaju sigurnosno-obavještajne agencije.[134]

Nadalje, zakonom je osnovano Vijeće za građanski nadzor sigurnosno-obavještajnih agencija u cilju ostvarivanja građanskog, odnosno neovisnog nadzora nad radom sigurnosnih službi.[135] U vezi s navedenim potrebno je istaknuti kako je „RH međunarodno prepoznata s inovativnim modelom građanskog nadzora nad dijelom sigurnosno-obavještajnog sustava kroz rad Vijeća za građanski nadzor sigurnosno-obavještajnih agencija. Rad ovoga Vijeća pokazao se uspješnim, te je u slučajevima u kojima je Vijeće donijelo zaključak bilo o nezakonitosti rada agencija, bilo o povredama ljudskih prava građana, uvijek došlo do unaprjeđenja rada čitavog sustava."[136] Vijeće je ovlašteno zaprimati predstavke građana/građanki, državnih tijela i pravnih osoba,[137] a radi provjere tvrdnji iznesenih u predstavci članovi Vijeća odlaze u nadzor agencija kako bi obavili neposredan uvid u službene zbirke podataka te u ostale relevantne činjenice.[138] Ako se utvrde nezakonitosti u postupanju agencija, predsjednik Vijeća o tome izvješćuje Predsjednika Republike Hrvatske, predsjednika Hrvatskoga sabora, predsjednika Vlade Republike Hrvatske, Glavnog državnog odvjetnika Republike Hrvatske i predsjednika Odbora za unutarnju politiku i nacionalnu sigurnost.[139]

ESLJP je u predmetima koji su se ticali tajnog nadzora i obavještajnog djelovanja države naveo zahtjev da mjere tajnog nadzora moraju biti podvrgnute neovisnom nadzoru kako bi bile u suglasnosti s EKLJP-om. Pri tome ESLJP ne zahtijeva da je taj nadzor nužno sudski u svim okolnostima,[140] iako daje prednost toj vrsti nadzora smatrajući sudstvo najboljim jamcem neovisnosti, nepristranosti i poštovanja postupovnih zahtjeva.[141] Iako nadzor rada sigurnosno-obavještajnih agencija u Hrvatskoj nije povjeren sudskoj vlasti, ona ipak djeluje kao pravni jamac i osigurava poštovanje postupovnih zahtjeva pri nalaganju mjera tajnog praćenja.[142] Nadalje, Hrvatski sabor kao tijelo koje obavlja nadzor rada sigurnosno-obavještajnih agencija u Hrvatskoj institucionalno je odvojeno tijelo i nezavisno od

[133] ZSOS, čl. 104.
[134] *Id.,* čl. 105.
[135] Zakonom o sigurnosnim službama RH od 28. ožujka 2002. propisano je osnivanje novog tijela - Vijeća za nadzor sigurnosnih službi, a Odlukom o Vijeću za nadzor sigurnosnih službi od 7. svibnja 2003. uređena su pitanja bitna za rad Vijeća koja nisu uređena Zakonom. Zakonom o sigurnosno-obavještajnom sustavu Republike Hrvatske od 17. svibnja 2006. izmijenjen je naziv Vijeća u Vijeće za građanski nadzor sigurnosno-obavještajnih agencija.
[136] Centar za mirovne studije, Gordan Bosanac, *Unaprjeđenje transparentnosti sigurnosno-obavještajnog sustava u RH,* str. 10, dostupno na http://www.cms.hr/system/publication/pdf/32/Policy_brief_SOA_final.pdf (pristup 7. travnja 2017.).
[137] Poslovnik o radu Vijeća za građanski nadzor sigurnosno-obavještajnih agencija, 2012, čl. 21.
[138] *Id.,* čl. 22.
[139] *Id.*, čl. 25.
[140] *Klass*, § 56.
[141] *Rotaru*, § 59.
[142] ZSOS, čl. 36., § 4.

sigurnosno-obavještajnih agencija nad kojima obavlja nadzor. Upravo su to zahtjevi koje je ESLJP stavio pred nesudski sustav nadzora rada obavještajnih tijela u Njemačkoj u predmetu *Klass.*[143] Daljnji zahtjev koji je sud stavio jest da su takvu tijelu osigurane dostatne ovlasti kako bi moglo izvršavati učinkovit i kontinuirani nadzor.[144] Iz gore navedenih odredaba zakona jasno je da je Hrvatskom saboru, odnosno Vijeću za građanski nadzor sigurnosno-obavještajnih agencija, dan velik broj ovlasti, uključujući i ovlast neposrednog nadzora i neposrednog uvida u službene zbirke podataka,[145] premda samo Vijeće opetovano traži da mu se osigura i „ovlast za obavljanje nadzora nad radom Operativno-tehničkog centra" kako bi Vijeće moglo u „potpunosti odgovoriti zahtjevima koji se pred njega postavljaju". [146]

3.1.3. Usporedni prikaz usklađenosti hrvatskog pravnog okvira sa zahtjevima ESLJP-a

ESLJP je u posljednje dvije godine donio dvije odluke u kojima je utvrdio povrede članka 8. EKLJP-a. Riječ je o predmetima *Roman Zakharov protiv Rusije*[147] i *Szabó i Vissy protiv Mađarske*.[148] Pred sudom je u ovom trenutku pet zahtjeva za odlučivanje o postojanju kršenja članka 8. EKLJP-a u kontekstu tajnog nadzora.[149] U nastavku dajemo prikaz nedostataka ruskog, odnosno mađarskog pravnog okvira koje je ESLJP našao u nesuglasju sa zahtjevima Konvencije usporedno s prikazom odredaba hrvatskog zakonskog okvira kojima se upravo osiguravaju pravna jamstva koja traži ESLJP.

Roman Zakharov protiv Rusije[150]	**Szabó i Vissy protiv Mađarske** [151]	**Pravni okvir sigurnosno-obavještajnog sustava Republike Hrvatske**
Pravni okvir osigurava obavještajnim, policijskim i drugim vlastima izravan pristup mobilnoj komunikaciji i povezanim podacima, bez	Nalaganje tajnih mjera u potpunosti je u nadležnosti izvršne vlasti.[153]	Nalog za tajno praćenje izdaje ovlašteni sudac Vrhovnog suda u formi pisanog obrazloženog naloga, a nalog (kao i prijedlog) mora sadržavati oznaku mjere koja će se primjenjivati, oznaku fizičke ili pravne osobe prema kojoj će se

[143] *Klass*, § 56.
[144] *Id.*
[145] Poslovnik o radu Vijeća za građanski nadzor sigurnosno-obavještajnih agencija, 2012, čl. 22.
[146] Izvješće Vijeća za 2011. godinu, dostupno na: http://www.sabor.hr/izvjesca (pristup 7. travnja 2017.).
[147] *Roman Zakharov protiv Rusije* (presuda), broj 47143/06, ESLJP 2015 [*Zakharov*].
[148] *Szabó i Vissy protiv Mađarske* (presuda), broj 37138/14, ESLJP 2016 [*Szabó*].
[149] *Centrum För Rättvisa protiv Švedske*, (zahtjev broj 35252/08); *Tretter i drugi protiv Austrije* (zahtjev broj 3599/10); *Bureau of Investigative Journalism and Alice Ross protiv Ujedinjenog Kraljevstva* (zahtjev broj 62322/14); *Human Rights Organisations and Others protiv Ujedinjenog Kraljevstva* (zahtjev broj 24960/15).
[150] U predmetu se radilo o sustavu tajnog nadzora mobilnih komunikacija te posebno o činjenici da su ruski teleoperateri bili obvezni instalirati uređaje i opremu koje su vlastima omogućavale direktan i neometan pristup komunikacijama korisnika, uz slaba ili gotovo nepostojeća pravna jamstva.
[151] Predmet je razmatrao u to vrijeme novi mađarski zakonodavni okvir za protuterorističko obavještajno djelovanje u povodu zahtjeva koji je naveo da je okvir pogodan za zlouporabu i kršenje ljudskih prava, prvenstveno iz razloga što nedostaje bilo kakav oblik sudske kontrole.
[153] *Szabó,* § 89.

potrebe dobivanja odobrenja od nadležne vlasti.[152]		mjera primjenjivati, obrazloženje razloga zbog kojih se mjera provodi i potrebe njezina poduzimanja te rok trajanja mjere. Ako se predlaže i dopušta poduzimanje više mjera, podaci za svaku mjeru moraju biti navedeni.[154]
Okolnosti u kojima je moguće poduzeti mjere tajnog nadzora nisu jasno navedene.[155]	Ne postoji test nužnosti temeljem kojeg se tajne mjere nalažu.[156]	Mjere tajnog prikupljanja podataka kojima se privremeno ograničavaju neka ustavna ljudska prava i temeljne slobode jesu *posljednje sredstvo* i mogu se koristiti samo ako se podaci ne mogu prikupiti na drugi način.[157]
	Zakonski okvir dopušta da gotovo bilo koja osoba (*virtually any person in Hungary*) bude podvrgnuta tajnom nadzoru, pa čak i osobe koje nisu predmet tajnih mjera.[158]	Nalog za poduzimanje mjere mora sadržavati, među ostalim, oznaku fizičke ili pravne osobe prema kojoj će se mjera primjenjivati.[159] Dokumenti o podacima koji se ne odnose na svrhu radi koje su prikupljani uništavaju se u roku od 30 dana.[160]
Najdulje trajanje mjera nije dostatno regulirano zbog nedostatka odredaba koje uređuju okolnosti prestanka mjere.[161]		Maksimalno trajanje mjera iznosi četiri mjeseca, a postupak za produljenje ili primjene novih mjera nad istom osobom stroži je te u njemu sudjeluje vijeće od tri ovlaštena suca Vrhovnog suda, koje je ovlašteno zatražiti dodatna mišljenja i obrazloženja, uključujući i od Vijeća za nacionalnu sigurnost.[162]
Domaći zakonodavni okvir dopušta automatsko pohranjivanje očigledno nebitnih podataka te ne sadrži jasne naznake okolnosti u kojima se presretani materijal pohranjuje i uništava.[163]		Dokumenti o podacima koji se ne odnose na svrhu radi koje su prikupljani, kao i podaci, dokumenti i informacije koji su prikupljeni na nezakonit način komisijski se uništavaju u roku od 30 dana.[164]
Sustav nadzora ne zadovoljava zahtjeve nezavisnosti, opsega	Zakonski okvir ne osigurava učinkovita	Hrvatski sabor, koji nadzor obavlja neposredno ili putem Ureda Vijeća

[152] *Zakharov,* §§ 269, 285, 302.
[154] ZSOS, čl. 36., § 4.
[155] *Zakharov,* §§ 229, 243, 302.
[156] *Szabó,* §§ 71-73.
[157] ZSOS, čl. 33.
[158] *Szabó,* §§ 66 i 89.
[159] ZSOS, čl. 36, § 4.
[160] *Id.*, čl. 41.
[161] *Zakharov,* §§ 186, 187, 250, 251.
[162] ZSOS, čl. 37.
[163] *Zakharov,* §§ 255, 302.
[164] ZSOS, čl. 41.

ovlasti i nadležnosti koje osiguravaju učinkovit i kontinuiran nadzor, kao ni zahtjev postojanja građanskog nadzora i učinkovitosti u praksi.[165]	pravna jamstva i pravne lijekove.[166]	za nacionalnu sigurnost i Vijeća za građanski nadzor sigurnosno-obavještajnih agencija,[167] institucionalno je odvojeno i nezavisno tijelo od sigurnosno-obavještajnih agencija nad kojima obavlja nadzor. Građanski nadzor nad radom sigurnosnih službi ostvaruje se putem Vijeća za građanski nadzor sigurnosno-obavještajnih agencija.[168]
Učinkovitost pravnih lijekova narušena je činjenicom odsutnosti obavijesti o postojanju tajnih mjera u bilo kojem trenutku, kao i nepostojanjem primjerenog pristupa dokumentima koji se odnose na postojanje tajnih mjere.[169]		Sigurnosno-obavještajne agencije dužne su na zahtjev građanina u roku od 15 dana obavijestiti ga pisanim putem jesu li prema njemu poduzimane mjere tajnog prikupljanja podataka te vode li se evidencije o njegovim osobnim podacima te mu na njegov zahtjev staviti na uvid dokumente o prikupljenim podacima.[170]

Iz svega navedenog možemo zaključiti kako je hrvatski pravni okvir sigurnosno-obavještajnog sustava u suglasju sa zahtjevima koje je ESLJP postavio odlučujući u predmetima koji su se ticali ograničavanja prava na privatnost u kontekstu obavještajnog nadzora.

3.2. Funkcioniranje u praksi sigurnosno-obavještajnog sustava RH

Funkcioniranje u praksi sigurnosno-obavještajnog sustava RH u kontekstu poštovanja ljudskih prava, kao i poštovanja gore navedenih zakonskih odredaba, naravno, teže je preispitati zbog potrebe da se očuva tajnim. Međutim javno dostupna izvješća Vijeća za građanski nadzor sigurnosno-obavještajnog sustava,[171] kao i javni dokument izdan 2014. godine od strane SOA-e, kojem je svrha bila „dati hrvatskoj javnosti bolji uvid u rad [SOA-e] i prikazati njegove rezultate“,[172] ipak donekle osvjetljavaju funkcioniranje u praksi

[165] *Zakharov,* §§ 272-285.
[166] *Szabó,* §§ 89, 48.
[167] ZSOS, čl. 104.
[168] Zakonom o sigurnosnim službama RH od 28. ožujka 2002. propisano je osnivanje novog tijela - Vijeća za nadzor sigurnosnih službi, a Odlukom o Vijeću za nadzor sigurnosnih službi od 7. svibnja 2003. uređena su pitanja bitna za rad Vijeća koja nisu uređena Zakonom. Zakonom o sigurnosno-obavještajnom sustavu Republike Hrvatske od 17. svibnja 2006. izmijenjen je naziv Vijeća u Vijeće za građanski nadzor sigurnosno-obavještajnih agencija.
[169] *Zakharov,* §§ 286-301, 302.
[170] ZSOS, čl. 40.
[171] Izvješća dostupna na: http://www.sabor.hr/izvjesca (pristup 6. travnja 2017.).
[172] Dokument dostupan na: https://www.soa.hr/UserFiles/File/pdf/JAVNI-DOKUMENT_web.pdf (pristup 6. travnja 2017.).

sigurnosno-obavještajnog sustava RH. U uvodnom obraćanju u predmetnom javnom dokumentu tadašnji je ravnatelj SOA-e naglasio kako „za obavljanje svojih zadaća, SOA ima značajne zakonske ovlasti koje ponekad zadiru i u ljudska prava te kako nadzor nad radom SOA-e smatra ključnim u osiguravanju da ona u potpunosti ispunjava svoju zakonsku ulogu i svoje ovlasti koristi isključivo u skladu sa zakonom.“ U kontekstu zaštite od nezakonitog zadiranja u Ustavom zajamčena ljudska prava, odnosno pravnog lijeka koji pojedinac može ishoditi putem alata koji su dostupni tijelima za nadzor sigurnosno-obavještajnog sustava, značajan je predmet S. B. pred Ustavnim sudom RH,[173] u kojemu je upravo mogućnost pojedinca da se predstavkom obrati Vijeću za građanski nadzor sigurnosno-obavještajnog sustava u slučaju sumnje u nezakonito zadiranje u Ustavom zajamčena ljudska prava dovelo do ostvarivanja pravne zaštite od ograničenja prava na privatnost, kao i ostvarivanja djelotvornog pravnog lijeka.

U tom je predmetu na temelju predstavke koju je podnositeljica, kandidatkinja za Savjet za razvoj civilnog društva, krajem siječnja 2007. podnijela Vijeću zbog sumnje da je nad njom izvršena nezakonita potpuna sigurnosna provjera Vijeće izradilo izvješće u kojem se, među ostalim, navodi: "Tijekom nadzora uočeno je da je s obzirom na provedbu potpune sigurnosne provjere bilo potrebno stvoriti Vam mogućnost za davanje suglasnosti za istu. U skladu s gore navedenim Vijeće smatra da je došlo do kršenja Ustavom zajamčenih ljudskih prava.“[174] Na temelju tog izvješća je krajem veljače 2007. Odbor za unutarnju politiku i nacionalnu sigurnost Hrvatskog sabora donio zaključak kojim je prihvatio Izvješće Vijeća kojim je utvrđeno kršenje Ustavom zajamčenih ljudskih prava i temeljnih sloboda kandidata za Savjet za razvoj civilnog društva iz razloga što je za kandidate napravljena potpuna sigurnosna provjera bez njihove suglasnosti, a tu je suglasnost trebao pribaviti Ured za udruge, tj. naručitelj sigurnosnih provjera.[175] Potom je podnositeljica predstavke 27. lipnja 2007. podnijela tužbu Općinskom građanskom sudu u Zagrebu protiv Ureda za udruge Vlade Republike Hrvatske i SOA-e, kojom je tražila da sud, među ostalim, utvrdi povredu prava na zaštitu i štovanje prava na osobni (privatni) život, zajamčenog člankom 35. Ustava RH i člankom 8. EKLJP-a. Postupak pred prvostupanjskim sudom, u kojem je odbačena tužba s obrazloženjem da ne postoje procesne pretpostavke da se tužiteljici pruži pravna zaštita, trajao je ukupno tri godine, dok je drugostupanjski sud nakon dvije godine potvrdio u bitnome presudu prvostupanjskog suda[176] te naveo kako „je pravilno utvrđeno da je provjera izvršena sukladno posebnim propisima koji to dopuštaju radi čega tužiteljica nije diskriminirana niti stavljena u nepovoljniji položaj u odnosu na druge građane RH, a niti su time prekršena njezina ljudska prava jer je člankom 33. stavkom 1. ZSOS-a propisano da SOA

[173] Ustavni sud Republike Hrvatske, odluka broj: U-III-164/2013 od 8. svibnja 2014. [*Odluka*].
[174] *Odluka,* str. 2.
[175] *Odluka,* str. 3.
[176] Drugostupanjski je sud utvrdio da nije bilo razloga za odbačaj tužbe, nego da je tužbu trebalo odbiti, no da takvo postupanje suda nije bilo na štetu podnositeljice.

može prema građanima primjenjivati mjere tajnog prikupljanja podataka kojima se privremeno ograničavaju neka ustavna ljudska prava i temeljne slobode."[177]

Ustavni je sud odlukom od 8. svibnja 2014. godine utvrdio da su odlukama prvostupanjskog i drugostupanjskog suda podnositeljici povrijeđena ljudska prava. Pozivajući se, među ostalim, na praksu ESLJP-a, Ustavni je sud utvrdio da je u predmetnom slučaju potpuna sigurnosna provjera predstavljala miješanje u prava podnositeljice na poštovanje privatnog života te kao takva predstavlja povredu članka 8. Konvencije i članka 35. Ustava, s obzirom na to da u domaćem zakonodavstvu koje je bilo na snazi u vrijeme provedbe sigurnosne provjere podnositeljice nisu postojala jamstva u odnosu na otklanjanje mogućih zlouporaba.[178] Ustavni je sud također utvrdio kako je očigledno da konkretni sudski postupak koji je podnositeljica inicirala zbog svoje dugotrajnosti ne predstavlja djelotvorno pravno sredstvo za zaštitu prava zajamčeno člankom 13. Konvencije, odnosno da on nije vođen na djelotvoran način, koji bi omogućio žuran prestanak nezakonite radnje i otklanjanje posljedica koje su iz nje nastale za podnositeljicu.[179]

Epilog te odluke Ustavnog suda jest i tužba koju je podnositeljica podnijela protiv Republike Hrvatske Općinskom građanskom sudu u Zagreb, temeljem koje **j**oj je, zbog utvrđene povrede prava na poštovanje privatnog i obiteljskog života, doma i dopisivanja, dosuđena odšteta od 20.000 kuna.[180] Iako presuda još nije pravomoćna, navedeni predmet primjer je funkcioniranja nezavisnog nadzora nad sigurnosno-obavještajnim sustavom u RH te postojanja i ostvarivanja pravnih jamstava i odgovarajuće pravne zaštite od ograničenja prava na privatnost u kontekstu nezakonitog poduzimanja mjera tajnog nadzora.

4. ZAKLJUČAK

Razmjerno je jasno da je praksa masovnog praćenja komunikacija od strane država postala globalna i svakidašnja pojava te da odista živimo u digitalnom dobu. Postavlja se pitanje jesu li uopće države međunarodnopravno legitimirane i uopće zainteresirane štititi svoje državljane od intruzija u njihovu komunikaciju ili bi pri takvu eventualnom pokušaju bile *estoppirane*[181] zbog globalno prisutne i globalno prihvaćene prakse mirnodopske špijunaže, ali i zbog činjenice da i same profitiraju od sustava za masovno praćenje komunikacija.

[177] *Odluka,* str. 7.
[178] *Id.,* str. 18.
[179] *Odluka,* str. 20.
[180] Centar za mirovne studije, *Aktivistkinji CMS-a odšteta zbog prisluškivanja: Neovisan nadzor nad sigurnosnim službama ključan za utvrđivanje povrede ljudskih prava,* 4. listopada 2016., dostupno na: http://www.cms.hr/hr/obavjestajne-sluzbe-soa/aktivistkinji-cms-a-odsteta-zbog-prisluskivanja-neovisan-nadzor-nad-sigurnosnim-sluzbama-kljucan-za-utvrdivanje-povrede-ljudskih-prava (pristup 6. travnja 2017.).
[181] Richard A. Falk, *Space Espionage and World Order: A Consideration of the Samos-Midas Program* u *Essays on Espionage and International Law*, 43, Roland J. Stanger (ur.), Columbus, 1962, str. 50.

Međutim poticaj da se pitanje mirnodopske špijunaže uredi međunarodnim pravom ne mora nužno doći od samih država, nego je moguće da do tog dođe zbog pritisaka pojedinaca koji su *de facto* pogođeni „špijunskim aktivnostima", barem kada je riječ o sustavima masovnog elektroničkog nadzora. Razlozi koji nas navode na taj zaključak jesu sljedeći. Djelovanje zviždača kao što je Edward Snowden već je prepoznato kao najdjelotvornije sredstvo za provođenje ograničenja obavještajnog djelovanja države iz razloga što, otkrivajući djelovanja država koja u današnje digitalno doba imaju globalni učinak, podižu svijest svjetske javnosti o postojanju i kršenju njihovih ljudskih prava. Iz tog razloga globalizacija može raditi i u korist globalne populacije, a ne samo u korist država i korporacija, jer se na neki način stvara „globalno civilno društvo", koje okuplja sve zainteresirane pojedince koji su odlučni boriti se za svoja prava. Pri tome pojedinci su prvenstveno upućeni na pravne alate: domaće sudove, kao i na međunarodne mehanizme za zaštitu ljudskih prava, te je upravo pravni pritisak jedan od načina na koji se može izvršiti pritisak na državu da mijenja svoje zakonodavne okvire u domeni obavještajnog djelovanja. Primjer za upravo navedeno jesu predmeti ESLJP-a protiv Ujedinjenog Kraljevstva koji su obrađivani u radu. Drugi je način politički, s kojim je nerijetko povezan i ekonomski pritisak. Primjere takva pritiska u kontekstu međudržavne špijunaže vidjeli smo upravo nakon Snowdenovih otkrića. Međutim i pojedinci su u mogućnosti izvršiti takav utjecaj izražavanjem neslaganja s politikom države na način da sabotiraju proizvode i usluge kojima se predmetna politika provodi ili s kojom su usko povezani. Zahvaljujući upravo digitalnom dobu, takve su akcije ne samo moguće nego i krajnje uspješne. Recentni primjer za to jest izražavanje neslaganja s politikom nove američke administracije svojevrsnim „kažnjavanjem" jednog od savjetnika u Vladi, glavnog izvršnog direktora *Ubera,* kompanije u vlasništvu koje je istoimeni globalni servis za dijeljenje prijevoza. Globalna akcija[182] *#DeleteUber*, u kojoj su korisnici uklanjali mobilnu aplikaciju *Uber* te prestali koristi uslugu u znak protesta, primorala je glavnog izvršnog direktora *Ubera* da odstupi s pozicije.[183]

Uzmemo li u obzir i duboko isprepletene odnose politike i gospodarstva te upućenost na njihovu vječnu simbiozu, ekonomski modeli i principi poput osluškivanja bila tržišta mogu biti preneseni i na politike država, posebice kada tržište „pokaže zube" te ugrozi ekonomsku stabilnost države. A tržište čine oni isti pojedinci koji su pogođeni masovnim nadzorom. Vezano uz politički pritisak na države, spomenimo i djelovanje tijela međunarodnih organizacija, posebice Odbora za prava čovjeka i Europskog parlamenta, predstavničkog tijela građana EU-a, koji ne samo da prokazuju sporne prakse država, čime također podižu svijest građana o kršenju njihovih prava, nego i daju mišljenja i smjernice državama kako ispraviti sporne prakse. U navedenom smjeru ide i zaključak Odbora za prava čovjeka, koji u svojem *Izvještaju o pravu na privatnost* potiče države da preispitaju

[182] Akcija je provođena ponajprije na području SAD-a, ali zbog globalne dostupnosti aplikacije, kao i zbog neslaganja s politikom nove administracije diljem svijeta, akcija je poprimila globalne razmjere.

[183] The Forbes, *Here's The Full Letter Uber's CEO Sent When He Quit Trump's Advisory Council,* 2. veljače 2017., dostupno na: http://www.forbes.com/forbes/welcome/?toURL=http://www.forbes.com/sites/briansolomon/2017/02/02/uber-ceo-quits-trump-advisory-council-after-deleteuber/&refURL=https://www.google.hr/&referrer=https://www.google.hr/ (pristup 9. veljače 2017.).

svoje zakonodavne okvire i uvrste učinkovita pravna jamstva kao žurnu mjeru osiguranja prava na privatnost.[184] Iste vrste pritiska mogle bi uroditi plodom i po pitanju uskraćivanja pravne zaštite strancima izbjegavanjem ekstrateritorijalne primjene instrumenata za zaštitu ljudskih prava, upravo kad se uzme u obzir da živimo u digitalnom dobu, koje briše državne granice. Čak je i SAD, najveći oponent takve primjene, nakon Snowdenovih otkrića priznao da je povjerenje svjetske javnosti od važnosti i utjecaja na provođenje američke politike.[185]

Digitalno doba u kojem živimo nosi nove životne i pravne izazove dajući nove dimenzije određenim ljudskim pravima i relativizirajući uvriježene međunarodne pojmove i institute, kao što je teritorijalna cjelovitost i efektivna kontrola u fizičkom smislu. Razvidno je da međunarodno pravo kaska za fenomenima koje digitalno doba izaziva, djelomično moguće i zbog tromosti međunarodne zakonodavne djelatnosti (ako je tako možemo nazvati), u kojoj glavnu riječ još uvijek imaju države kao jedini nesporni subjekti međunarodnog prava. Iz tog je razloga potrebno aktivirati mehanizme unutarnjeg pritiska, pravnog i političkog, kako bi oni potaknuli djelovanje država na međunarodnom planu u pravcu ograničavanja masovnog nadzora, koji je, pokazalo se, izvan svake kontrole.

[184] *Izvještaj*, § 50.
[185] *Govor Obama.*

INTERNATIONAL LEGAL IMPLICATIONS OF PEACETIME ESPIONAGE IN THE FORM OF MASS ELECTRONIC SURVEILLANCE IN THE HUMAN RIGHTS CONTEXT AND AN EVALUATION OF THE CROATIAN LEGAL FRAMEWORK FOR SURVEILLANCE

The aim of this paper is to provide an overview of the international legal implications of peacetime espionage in the form of mass electronic surveillance. This subject was provoked by the publication of leaked official secret documents revealing the magnitude of mass electronic surveillance run by States that were abusing the technological complexities of global data transmission while taking advantage of the lack of international law regulation of peacetime espionage. The paper includes an analysis of the consequential key legal issues of the legal relationship arising between a State that undertakes such surveillance and an individual who is being targeted. This relationship falls within the scope of human rights. Therefore, the paper examines the case law of international mechanisms for the protection of human rights, especially the case law of the European Court of Human Rights. The case law is then placed against the Croatian legal framework for secret surveillance in order to determine its compliance with the demands of the legality of interference with the right to privacy in the digital age.

Keywords: *mass electronic surveillance, right to privacy, Croatian legal framework for surveillance*

Zrinka Salaj, Ministry of Justice of the Republic of Croatia, attending the postgraduate doctoral study programme in International Public and Private Law at the Faculty of Law, University of Zagreb