УДК: 355.40:004.738.5
DOI: https://doi.org/10.22182/pnb.2212022.9
Прегледни рад

Политика националне безбедности
Година XIII, vol. 22
број 1/2022.
стр. 189-209

Синиша Домазет*

Факултет за студије безбедности, Универзитет Едуконс, Сремска Каменица

САЈБЕР ШПИЈУНАЖА И ПРАВО НА ПРИВАТНОСТ СА АСПЕКТА ДОСАДАШЊЕ ПРАКСЕ ЕВРОПСКОГ СУДА ЗА ЉУДСКА ПРАВА И УЈЕДИЊЕНИХ НАЦИЈА

Сажетак

Сајбер шпијунажа у XXI веку представља изазов у међународним односима, као и њена веза са људским правима, превасходно правом на приватност. Предмет истраживања је анализа међусобног односа између делатности савремених обавештајних служби и њиховог настојања да заштите националну безбедност с једне стране и потребе да се заштити право на приватност с друге стране. Утврђено је да се право на приватност под одређеним околностима може ограничити. Акти Уједињених нација и јуриспруденција Европског суда за људска права дефинисали су одговарајуће стандарде при процени легалности ограничења права на приватност. Истраживање је показало да оспорена мера мора имати основу у домаћем праву. Даље, закон треба да буде приступачан датом лицу, које мора бити у стању да предвиди његове последице по њега. Мора се обезбедити и да се мере тајног надзора примењују само када су неопходне у демократском друштву посебно обезбеђивањем адекватних и делотворних заштитних механизама и гаранција против злоупотреба. У сваком случају понаособ потребно је одмерити пропорционалност мере надзора са обимом ограничења права на приватност, као и да постоји легитимни циљ за тако нешто. У истраживању су коришћени нормативни метод и правно-логички методи индукције и дедукције.

* Контакт: sdomazetns@gmail.com
ORCID iD: https://orcid.org/0000-0002-5964-2249

Кључне речи: право, безбедност, сајбер простор, масовни надзор, обавештајне службе

УВОД

Развој информационо-комуникационих технологија донео је са собом многобројне позитивне ствари и промене у читавом свету, у свим сегментима живота и рада. Интернет је постао неизоставни део живота већине људи и из године у годину шири се број корисника у свим деловима света. Према најновијим подацима, у првом кварталу 2021. године, преко пет милијарди становника планете (односно 65% популације) има приступ Интернету, што чини раст од преко 1300% у односу на 2020. годину (Internet World Stats 2021). У времену које следи, поменуте бројке ће свакако бити веће, посебно с обзиром на развој Интернета интелигентних уређаја (енг. *Internet of Things*), вештачке интелигенције и блокчејн (енг. *Blockchain*) технологија.

Показало се да је сајбер простор изузетно користан за повезивање људи, размену идеја, знања и искуства. Међутим, појавиле су се и мрачне стране интернета, који је постао плодно тло за многобројне облике злоупотреба и претњи. Притом, угрожени субјекти нису само обични грађани и привреда који користе интернет, већ и субјекти од значаја за националну безбедност. Временом су претње постајале све софистицираније и вишезначне, па се почело говорити о сајбер претњама које потичу од хактивизма, сајбер вандализма, сајбер криминала, сајбер тероризма, сајбер напада против критичне инфраструктуре, сајбер превара финансијске природе, па све до сајбер шпијунаже и сајбер рата (Goldman and McCoy 2016, 595-597). Наведени облици претњи у великом броју случајева са собом носе и додатну опасност по личне податке и приватност грађана широм света, нарочито уколико претња потиче од органа јавне власти, или субјеката под њеном контролом.

У овом раду ће пажња посебно бити усмерена на сајбер шпијунажу, која у XXI веку представља прави изазов у међународним односима, као и њену везу са људским правима, превасходно правом на приватност. Разлога за то није мало. Једна од главних прекретница представља случај бившег припадника америчке Агенције за националну безбедност (NSA) Едварда Сноудена. Наводи Сноудена у погледу делатности америчког обавештајног сектора су пробудили донекле успавану међународну јавност по питању заштите права на приватност, односно личних података грађана широм света. Ситуацију додатно усложњава и чињеница да све више земаља

поседује техничко знање и капацитете за извођење најразличитијих облика сајбер шпијунаже, при чему професионализам на овом пољу расте из дана у дан, посебно кад су у питању велике силе. Различита техничка достигнућа и поседовање могућности за њихово коришћење, понекад у неслућеним границама, довели су до тога да се почело прибегавати масовном сајбер (онлајн) надзору комуникација и свакодневног живота грађана, не водећи притом довољно рачуна о загарантованим слободама и правима грађана.

Дакле, предмет рада је анализа међусобног односа између делатности савремених обавештајних служби и њиховог настојања да заштите националну безбедност с једне стране, и потребе да се заштити право на приватност с друге стране. У првом делу рада биће више речи о појму сајбер шпијунаже и њеним појавим облицима, да би се потом прешло на анализу аката Уједињених нација и судске праксе Европског суда за људска права који се односе на заштиту права на приватност и услова под којима оно може бити ограничено, у циљу заштите националне безбедности.

ПОЈАМ САЈБЕР ШПИЈУНАЖЕ

Уколико се говори о шпијунажи, може се рећи да она, историјски гледано, представља један од најчешћих начина за прикупљање података политичког, економског или војног карактера, чији корени датирају још из периода старог Египта, античке Грчке, или старог Рима. Временом се ова делатност усавршавала у организационом, техничком и сваком другом погледу, тако да се данашње, модерне обавештајне службе у много чему разликују у односу на оне из ранијих историјских епоха. Како истиче Волфганг Кригер, у свом делу „Историја тајних служби: од фараона до НСА“, „сасвим је сигурно да се шпијун на бојном пољу Александра Великог Македонског тешко може свести на заједнички именилац са данашњом обавештајном делатношћу, која се ослања на компјутере и сателите. Па ипак, основни принципи политике, а понекад чак и војни принципи, веома развијених држава Антике и данашње политике били су веома слични. Исти је остао, пре свега, људски фактор“ (Кригер 2016).

Постоји много различитих дефиниција шпијунаже, при чему треба истаћи да међународно право не садржи неку општеприхваћену дефиницију. Заправо, постоји читаво шаренило дефиниција, посебно у правним системима држава широм света. На овом месту биће поменуте неке од њих. Тако, према неким ауторима, шпијунажа

представља „прибављање и одавање података који представљају неку тајну“ (Бошковић 2017). Постоје и дефиниције које шпијунажу одређују као „тајно, потајно, прикривено и на преваран начин прикупљање економских, политичких, војних и техничких података, које држава и покрети означавају као тајне“ (Тепавац 2019, 164), или као „свесно лажно прикупљање информација, које је наредила влада или организација која је непријатељска или сумњива према онима на које се информације односе, а које су извршили људи који нису овлашћени од стране мете за прикупљање“ (Demarest 1996, 325-326), док неки други аутори шпијунажу дефинишу као „прикупљање поверљивих информација без неопходне дозволе њиховог власника“ (Androulidakis and Fragkiskos-Kioupakis 2016).

Сајбер шпијунажа је релативно нов феномен, који се појавио и развијао упоредо са настанком и развојем Интернета и информационо-комуникационих технологија. Може се рећи да сајбер шпијунажа представља својеврсну продужену руку класичне шпијунаже, с обзиром на технике које се притом користе. Штавише, овај облик шпијунаже омогућава бројна преимућства у односу на класичну шпијунажу, с обзиром да се прибављене информације могу прикупљати на даљину (дакле, без коришћења људског фактора, уз ризик губитка или преврбовања агента), уз релативно мале трошкове (једна успешна сајбер шпијунска операција може донети нападачу огромну добит, односно огромну штету другој страни), неслућене брзине (брзина прибављања употребљивих информација је од кључне важности) и у великом обиму и временски неограничено (макар до откривања шпијунске сајбер операције од противника). Може се слободно тврдити да је XXI век „златно доба“ сајбер шпијунаже и све државе, посебно велике силе, радо прибегавају овом виду шпијунаже.

Сајбер шпијунажа се може одредити као „коришћење сајбер могућности за надгледање, праћење, хватање или ексфилтрирање електронски пренесених или ускладиштених комуникација, података или других информација“ (International Groups of Experts 2017), „коришћење радњи и операција-можда у дужем временском периоду-за прибављање информација које би се у супротном чувале поверљивим и које се налазе на или пролазе кроз противничке компјутерске системе или мреже“ (Lin 2010, 63), „чин или пракса прибављања тајне (осетљиве, власничке или поверљиве информације) од појединаца, конкурената, ривала, група, влада и непријатеља за војну, политичку или економску предност, користећи илегалне методе истраживања унутар Интернета, мреже, софтвера и/или

рачунара“ (Coleman 2008), или „наука о тајном хватању саобраћаја е-поште, текстуалних порука, других електронских комуникација и корпоративних података у сврху прикупљања података о националној безбедности или комерцијалних обавештајних информација“ (Kilovaty 2016, 47).

Британска влада у Националној стратегији за сајбер безбедност од 2016-2021. године у речнику појмова сајбер шпијунажу изједначава са појмом „експлоатација рачунарске мреже“ (енг. “*Computer Network Exploitation*”), истичући да се под тим појмом подразумева „коришћење рачунарске мреже за инфилтрирање у циљану рачунарску мрежу и прикупљање обавештајних података“ (UK HM Government 2016). С друге стране, у посебној америчкој председничкој директиви PPD-20 о америчкој политици сајбер операција се појам сајбер шпијунаже изједначава са појмом „сајбер прикупљања“ (енг. “*Cyber collection*”), наводећи да се ради о „операцијама и сродним програмима или активностима које се спроводе од стране Владе Сједињених Држава или у њено име, у или преко сајбер простора, за примарну сврху прикупљања обавештајних података-укључујући информације које се могу користити за будуће операције-од рачунара, информационих или комуникационих система, или мрежа са намером да се остане неоткривен“ (President of the United States, PPD-20).

Кинеска управа за сајбер безбедност у Националној стратегији за сајбер простор из 2016. године не даје стриктну дефиницију овог појма, али истиче да „употреба мрежа за мешање у унутрашње политичке послове других земаља, за напад на политичке системе других земаља, подстицање социјалних немира, подривање режима других земаља, као и сајбер надзор великих размера, сајбер шпијунажа и друге сличне активности наносе озбиљну штету националној политичкој безбедности и информационој безбедности корисника“ (Cyberspace Administration of China 2016).

Дакле, сајбер шпијунажа је вишеслојан појам и за очекивати је да ће се у наредном периоду, са даљим развојем информационо-комуникционих технологија, он даље проширивати.

ПОЈАМ И ОГРАНИЧЕЊА ПРАВА НА ПРИВАТНОСТ

Појам приватности је дуго био предмет великог броја расправа и заокупљао је пажњу не само научне и стручне јавности и медија, већ и грађана широм света. Убрзани развој интернета, блокчејн технологија, интернета интелигентних уређаја, као и вештачке

интелигенције додатно је повећао бриге у вези са очувањем безбедности грађана и поставио нове захтеве у вези обухвата права на приватност. Кад је реч о дефиницији приватности, може се уочити велики број различитих приступа.

Тако, може се поменути дефиниција појединих аутора која право на приватност одређује као „право на спречавање ризика, или смањење ризика на прихватљив ниво да један субјект користи туђе приватне информације, а да за то нема овлашћење" (Бошковић 2017). Неке дефиниције под приватношћу су подразумевале „личну аутономију, демократску партиципацију, управљање сопственим идентитетом и друштвену координацију" (Cho, Rivera-Sanches and Sun Sun 2009, 395-416). У литератури је могуће пронаћи и појам „приватности у електронским комуникацијама", која обухвата „прикупљање, обраду и давање информација о кориснику трећим лицима, при чему појединци/појединке када бележе активности и личне податке сами одређују када, како и у којој мери информације о њиховој приватној сфери треба и могу да буду доступне другима" (Јовановић, 2014, 94, цитирано у: Вилић, 2016, 20). Има и аутора који користе појам „информациона приватност", под којом подразумевају захтев појединаца, група или институција да самостално одлуче када ће, како и које информације о себи уступити другима. Према њима, у ширем смислу, појам информационе приватности обухвата „информациону сигурност, што подразумева да појединац у условима постојања информационог друштва одлучује када, коме, колико и како ће да саопшти личне податке, водећи рачуна о својим правима и потребама, као и о правима и потребама заједнице у којој живи. Информациона приватност обједињује правне вредности заштите права појединаца у друштву развијених информационих технологија, а овај концепт заштите личних података, везан за комуникацију преко електронских мрежа, другачије се назива и "е-приватност" (Boban, 2012, 581-582,595).

Право на приватност је било предмет разматрања и од стране међународних организација. На овом месту се може поменути став Савета за људска права УН, као и Генералне Скупштине УН из 2013. године, да државе имају обавезу да „поштују и штите право на приватност, укључујући и у контексту дигиталне комуникације" (United Nations General Assembly 2013). Сличан став заузет је и 2015. године, где је истакнуто да „иста права која људи имају ван мреже такође морају бити заштићена на мрежи, укључујући право на приватност" (United Nations General Assembly 2015). На овом месту треба поменути и члан 12. Универзалне декларације УН о

људским правима из 1948. године, где се наводи да се „нико не сме изложити произвољном мешању у приватни живот, породицу, стан или преписку, нити нападима на част и углед. Свако има право на заштиту закона против оваквог мешања или напада“. Међународни пакт о грађанским и политичким правима из 1966. године у члану 17. такође наводи да „нико не може бити предмет самовољних или незаконитих мешања у његов приватни живот, у његову породицу, у његов стан или његову преписку, нити незаконитих повреда нанетих његовој части или његовом угледу“. У члану 8. Европске конвенције за заштиту људских права и основних слобода из 1950. године истиче се да „свако има право на поштовање свог приватног и породичног живота, дома и преписке“.

Нарочито важан став видљив је у Коментару Високог комесара УН за људска права из 1988. године, где је у пар. 8. истакнуто да „надзор, било електронски или други, пресретање телефонских, телеграфских и других облика комуникације, прислушкивање и снимање разговора треба забранити“ (Office of the High Commissioner for Human Rights 1988). Такав став је потврђен у пракси од стране Европског суда за људска права у случају *Liberty and Others v. the United Kingdom* из 2008. године, где се наводи да су „комуникације телефоном, факсом и е-поштом обухваћене појмовима „приватни живот“ и „преписка“ у смислу члана 8. (Европске конвенције о заштити људских права и основних слобода, прим. С.Д). Суд подсећа на своје налазе у претходним предметима [...] да само постојање закона који дозвољава систем за тајно праћење комуникација подразумева претњу надзора за све оне на које се закон може применити. Ова претња нужно погађа слободу комуникације између корисника телекомуникационих услуга и самим тим представља мешање у остваривање права подносилаца представке према члану 8, без обзира на све мере предузете против њих“ (*Case of Liberty and Others v. the United Kingdom*, 58243/00, par. 56). На основу наведеног, јасно је да прикупљање поверљивих информација и пресретање приватних комуникација (без обзира на средство) од стране државе представља кршење права на приватност.

У погледу националних прописа којима се уређује право на приватност, могу се уочити различити приступи. Тако, у неким државама је право на приватност наведено, односно експлицитно признато у уставима тих земаља. Друго, постоје и државе где је право на приватност посредно (индиректно) регулисано уставом, као и прописима из области кривичног законодавства (пример су САД). Треће, многе државе су донеле посебне прописе којима се

уређује заштита података о личности, док у неким земљама право на приватност није признато као аутономно право (примера ради, у Уједињеном Краљевству и Кини) (Домазет и Динић 2022, у штампи).

С обзиром на сву сложеност овог појма и изазове које су с тим у вези донеле нове технологије, не треба да чуди што су различита тела која се баве заштитом људских права избегавала да прецизно дефинишу појам права на приватност. Штавише, може се рећи да се у јуриспруденцији појам приватности схвата доста широко, што потврђују одређени случајеви. На пример, у случају *Mikulić v. Croatia*, Европски суд за људска права је у својој пресуди истакао да "поштовање приватног живота захтева да сви треба да буду у стању да утврде детаље свог идентитета као појединачна људска бића и да је право појединца на такве информације од важности због његових импликација на његову личност" (*Case Mikulić v. Croatia*, 53176/99, par. 54), док је у случају *Pretty v. United Kingdom* истакао да је „концепт „приватног живота" широк појам који није подложан исцрпној дефиницији. Покрива физички и психички интегритет особе. Понекад може да обухвати аспекте физичког и друштвеног идентитета појединца. Елементи као што су, на пример, родна идентификација, име и сексуална оријентација и сексуални живот спадају у личну сферу, у складу са чланом 8 (Европске конвенције о заштити људских права и основних слобода, прим. С.Д). Члан 8. такође штити право на лични развој и право на успостављање и развијање односа са другим људским бићима и спољним светом. Иако ниједан претходни случај није као такав утврдио право на самоопредељење које је садржано у члану 8. Конвенције, Суд сматра да је појам личне аутономије важан принцип који лежи у основи тумачења његових гаранција" (*Case Pretty v. United Kingdom Judgment*, 2346/02, par. 61).

Важан је и случај *Shimovolos v. Russia*, где је Европски суд за људска права указао да „члан 8. није ограничен на заштиту „унутрашњег круга" у којем појединац може да живи свој лични живот како жели и да из њега у потпуности искључи спољашњи свет који није обухваћен тим кругом. Такође штити право на успостављање и развијање односа са другим људским бићима и спољним светом. Приватни живот може чак укључивати активности професионалне или пословне природе" (*Case Shimovolos v. Russia Judgment*, 30194/09, par. 64). Даље, у истој пресуди наводи се да је „систематско прикупљање и чување података од стране служби безбедности о одређеним лицима представљало мешање у приватни живот ових лица, чак и ако су ти подаци прикупљени на јавном месту,

или се тичу искључиво професионалних или јавних активности особе“ (*Case Shimovolos v. Russia Judgment*, 30194/09, par. 65).

Без обзира на важност и многобројне дефиниције, право на приватност не представља апсолутно право, што значи да под одређеним условима оно може бити ограничено. О томе посебно говори члан 8. Европске конвенције о заштити људских права и основних слобода. У поменутом члану се наводи да се „јавне власти неће мешати у вршење овог права, сем ако то није у складу са законом и неопходно у демократском друштву у интересу националне безбедности, јавне безбедности или економске добробити земље, ради спречавања нереда или криминала, заштите здравља или морала, или ради заштите слободе и права других“. С друге стране, у Међународном пакту о грађанским и политичким правима се у члану 17. истиче да „нико не може бити предмет самовољних или незаконитих мешања у његов приватни живот“. Занимљиво је поменути и становиште Комитета за људска права УН (Генерални коментар број 27), где се у пар. 11. наводи да „ограничења (права на приватност, прим. С.Д.) морају бити предвиђена законом, морају бити неопходна у демократском друштву“ (Human Rights Committee 1999).

Још значајнија одредба садржана је у пар. 28. Извештаја Високог Комесара УН за људска права из 2014. године, према коме „држава мора да обезбеди да је свако мешање у право на приватност, породицу, дом или преписку допуштено законима који (а) су јавно доступни; (б) садрже одредбе које обезбеђују да је прикупљање, приступ и коришћење комуникационих података прилагођено одређеним легитимним циљевима; (ц) су довољно прецизни, детаљно наводећи прецизне околности у којима такво мешање може бити дозвољено, процедуре за давање овлашћења, категорије лица која могу бити стављена под надзором, ограничења трајања надзора и процедуре за коришћење и чување прикупљених података; и (д) обезбеди ефикасне мере заштите од злоупотребе“ (United Nations General Assembly 2014).

На овом месту треба нагласити и велики значај судске праксе Европског суда за људска права, која је дефинисала одговарајуће стандарде при процени легалности ограничења права на приватност. Тако, у случају *Weber and Saravia v. Germany*, Суд је заузео став да мера ограничења права на приватност мора бити у складу са правом, а под тим изразом се у случају *Szabo and Vissy v. Hungary* наводи да „прво, оспорена мера мора да има неку основу у домаћем праву; такође се односи на квалитет дотичног закона, захтевајући да треба

да буде компатибилан са владавином права и приступачан датом лицу, који, штавише, мора бити у стању да предвиди њене последице по њега. „Квалитет права“ у овај смисао имплицира да домаће право не само да мора бити доступно и предвидљиво у својој примени, већ мора обезбедити и да се мере тајног надзора примењују само када су „неопходне у демократском друштву“, посебно обезбеђивањем адекватних и делотворних заштитних механизама и гаранција против злоупотреба“ (Case of Szabo and Vissy v. Hungary, 37138/14, par. 59).

У погледу доступности домаћег права, у већ поменутом случају *Shimovolos v. Russia*, указано је да закон треба да је „доступан дотичном лицу, које мора, штавише, бити у стању да предвиди његове последице по њега“ (*Case Shimovolos v. Russia Judgment*, 30194/09, par. 67). Овај захтев је нарочито важан када се говори о обавештајним службама, с обзиром на природу њихове делатности. С тим у вези, обавештајне службе махом желе да избегну да се њихова делатност и овлашћења прецизно уреде законским прописима донетим у парламенту. Штавише, њихова делатност је, неретко, уређена актима интерног и неформалног карактера, у оквиру владиних тела. Управо у вези са овим посебно долази до изражаја пар. 29. Извештаја Високог Комесара УН за људска права из 2014. године, где се истиче да „последично, тајна правила и тајна тумачења – чак и тајна судска тумачења – права немају потребне квалитете закона“ (United Nations General Assembly 2014). Из овога се може закључити да се обавештајним службама не смеју дати превелика дискрециона овлашћења, с обзиром на значајне могућности злоупотреба. Стога се морају ограничити и јасно прецизирати овлашћења обавештајних агенција, при чему прописи морају бити транспарентни и доступни грађанима, а не скривени од очију јавности.

Потом, прописи морају бити таквог карактера да је могуће предвидети ефекте њихове примене. Тачније речено, грађани морају да буду у стању да разумеју под којим условима и околностима обавештајне службе могу предузимати мере надзора над њиховим активностима. Да би се то постигло, прописи морају бити довољно прецизни, како не би долазило до различитих тумачења, са несагледивим последицама.

С тим у вези, посебно је интересантан случај *Roman Zakharov v. Russia* из 2016. године, у коме је проблем представљало тајно пресретање мобилних телефонских комуникација. У том случају, Европски суд за људска права је заузео став да „позивање на „предвидљивост” у контексту пресретања комуникација не може бити исто као у многим другим областима. Предвидљивост у

посебном контексту тајних мера надзора, као што је пресретање комуникација, не може значити да би појединац требало да буде у стању да предвиди када ће власти вероватно пресрести његову комуникацију како би он могао да прилагоди своје понашање у складу са тим [...]. Домаћи закон мора бити довољно јасан да грађанима пружи адекватну индикацију у вези са околностима и условима под којима су јавни органи овлашћени да прибегну таквим мерама" (*Case Roman Zakharov v. Russia*, 47143/06, par. 229). Даље, у истој пресуди наведено је да „с обзиром да примена мера тајног надзора комуникација у пракси није под надзором појединаца или јавности у целини, било би у супротности са владавином закона да се дискреционо право дато извршној власти или судији да изразити у терминима неспутане моћи. Сходно томе, закон мора назначити обим сваког таквог дискреционог права датог надлежним органима и начин његовог коришћења са довољном јасноћом да се појединцу пружи адекватна заштита од произвољног мешања. (*Case Roman Zakharov v. Russia*, 47143/06, par. 230).

Такође, Суд је заузео став и да „захтев „предвидивости" закона не иде толико далеко да приморава државе да донесу законске одредбе које детаљно наводе сва понашања која могу довести до одлуке да се појединац подвргне тајном надзору из разлога „националне безбедности". По својој природи, претње националној безбедности могу се разликовати по карактеру и могу бити неочекиване или тешко унапред дефинисане [...]. Закон мора довољно јасно да назначи обим сваке такве дискреционе слободе која је дата надлежним органима и начин њеног спровођења, имајући у виду легитимни циљ дотичне мере, да се појединцу пружи адекватна заштита од произвољног мешања" (*Case Roman Zakharov v. Russia*, 47143/06, par. 247).

Занимљиво је поменути и случај *Weber and Saravia v. Germany*, где је Суд поставио одређене „минималне мере заштите које би требало да буду постављене [...] како би се избегле злоупотребе овлашћења: природа кривичних дела која могу довести до налога за пресретање; дефиниција категорија људи којима се прислушкују телефони; ограничење трајања прислушкивања телефона; поступак који треба следити за испитивање, коришћење и чување добијених података; мере предострожности које треба предузети приликом саопштавања података другим странама; и околности у којима снимци могу или морају бити избрисани или траке уништене" (*Case Weber and Saravia v. Germany*, 54934/00, par. 95).

Даље, национално законодавство мора бити формулисано на начин да се спрече могуће злоупотребе приликом спровођења мера

сајбер шпијунаже, односно сајбер надзора. Одређене недоумице у вези са овим проблемом разрешила су тела Уједињених Нација, а одговарајући ставови заузети су и од стране Европског суда за људска права. Кад је реч о Уједињеним Нацијама, значајно је споменути активност Генералне скупштине УН, која је још 2016. године заузела став да су државе обавезне да „успоставе или одржавају постојеће независне, ефективне, адекватним ресурсима и непристрасним судским, административним и/или парламентарним домаћим механизмима надзора који могу осигурати транспарентност, а према потреби, и одговорност за државни надзор комуникација, њихово пресретање и прикупљање личних података“ (United Nations General Assembly 2016).

Кад је реч о судској пракси Европског суда за људска права, у случају *Klass and Others v. Germany*, заузет је став да се „суд мора уверити да, који год систем надзора буде усвојен, постоје адекватне и делотворне гаранције против злоупотребе. Ова процена има само релативан карактер: зависи од свих околности случаја, као што су природа, обим и трајање могућих мера, разлога потребних за наређивање таквих мера, надлежни органи да дозволе, спроводе и надгледају такве мере и врсту правног лека предвиђеног националним законом“ (*Case Klass and Others v. Germany*, 5029/71, par. 50).

У случају *Weber and Saravia v. Germany*, Суд је истакао да је „питање накнадног обавештавања о надзорним мерама нераскидиво повезано са делотворношћу правних лекова пред судовима, а самим тим и са постојањем ефективних заштитних механизама против злоупотребе овлашћења надзора, пошто у принципу постоји мало простора за прибегавање судовима од стране дотичног појединца, осим ако је потоњи обавештен о мерама предузетим без његовог знања и на тај начин може ретроспективно да оспори њихову законитост“ (*Case Weber and Saravia v. Germany*, 54934/00, par. 135).

Важан је и случај *Szabó and Vissy v. Hungary*, где је Суд навео да „владавина права подразумева, између осталог, да мешање извршне власти у права појединца треба да буде предмет ефективне контроле коју би обично требало да обезбеди правосуђе, барем у крајњем случају, нудећи судску контролу најбоље гаранције независности, непристрасности и правилног поступка. У области у којој је злоупотреба потенцијално тако лака у појединачним случајевима и може имати тако штетне последице по демократско друштво у целини, у принципу је пожељно да се надзорна контрола повери судији“ (*Case Szabo and Vissy v. Hungary*, 37138/14, par 77).

Међутим, пракса Суда за људска права, што је показано у пар. 56. у одлуци у случају *Klass v. Germany*, допушта и могућност да се контрола повери и несудским телима, под условом да су она „независна од органа који спроводе надзор и да имају довољна овлашћења и надлежности да врше ефикасну и континуирану контролу". То не значи да ће свако несудско тело, као на пример министар правде, бити довољна гаранција непристрасности и независности у надзору, што је потврђено у поменутом пар. 77. одлуке у случају *Szabó v. Hungary*. Дакле, ово питање ће се процењивати у сваком случају понаособ.

Ограничења права на приватност могућа су и у случају да постоји одговарајући легитимни циљ за такву активност, о чему посебно говори члан 8(2) Европске конвенције о заштити основних права и људских слобода. Судска пракса Европског суда за људска права и у овом случају потврдила је наводе из члана 8. Конвенције.

Тако, у већ поменутом случају *Klass v. Germany*, Суд је заузео становиште да „држава мора бити у стању, да би се ефикасно супротставила [...] претњама, да предузме тајни надзор субверзивних елемената који делују у оквиру њене надлежности. Суд стога мора да прихвати да је постојање неког закона који даје овлашћења тајног надзора над поштом, поштом и телекомуникацијама, под изузетним условима, неопходно у демократском друштву у интересу националне безбедности и/или ради спречавања нереда или злочина" (*Case Klass and Others v. Germany*, 5029/71, par. 48).

Посебно је с овим у вези занимљив поменути случај *Szabó v. Hungary*, где је Суд окарактерисао важеће мађарске прописе у вези са надзором као незаконите, јер је постојала могућност да надлежна тела донесу одлуке о спровођењу мера надзора без обавезе да „произведу пратеће материјале или, посебно, довољну чињеничну основу за примену мера тајног прикупљања обавештајних података која би омогућила процену неопходности предложене мере - и то на основу индивидуалне сумње у вези са циљаном особом" (*Case Szabo and Vissy v. Hungary*, 37138/14, par 71). У пракси Суда су се искристалисали и ставови да су "овлашћења тајног надзора над грађанима, која карактеришу и полицијску државу, подношљива према Конвенцији само у мери у којој је то неопходно за очување демократских институција" (*Case Klass and Others v. Germany*, 5029/71), односно да „надзорно тело мора бити у стању да провери постојање основане сумње против дотичне особе, посебно да ли постоје чињеничне индиције за сумњу да је то лице планирало, починило или да је извршило кривична дела или друга дела која

могу довести до мера тајног надзора, као што су као на пример дела која угрожавају националну безбедност“ (*Case Roman Zakharov v. Russia*, 47143/06).

Дакле, да би се право на приватност могло ограничити коришћењем мера сајбер шпијунаже, потребно је да постоји и легитимни циљ за тако нешто. Остаје дилема шта чинити у случају када, приликом спровођења мера надзора над осумњиченим лицима, дође до случајног прикупљања личних података невиних грађана. С тим у вези, као услов за ограничење права на приватност стоји и принцип пропорционалности. Пракса Европског суда за људска права потврдила је овај став у већ помињаном случају *Weber and Saravia v. Germany*, када је Европски суд за људска права заузео став да је „спорна одредба била неопходна у демократском друштву. Успоставила је одговарајућу равнотежу између јавног интереса у отклањању озбиљних опасности [...] и интереса особа на које мере праћења утичу“ (*Case Weber and Saravia v. Germany*, 54934/00, par. 108).

Анализом судске праксе може се закључити да је неопходно у сваком случају понаособ одмерити пропорционалност мере надзора са обимом ограничења права на приватност. Уколико се утврди да се легитимни циљ националне безбедности могао остварити мерама или средствима која су мање рестриктивна у односу на ограничење људских права, односно права на приватност, тада ће се радити о незаконитој делатности. Разуме се, остаје дилема колика ће маргина процене у сваком конкретном случају у пракси бити примењена од стране држава.

МАСОВНИ НАДЗОР У ПРАКСИ ЕВРОПСКОГ СУДА ЗА ЉУДСКА ПРАВА

Злоупотреба сајбер технологија, нажалост, поприма све озбиљније размере, а показало се да масовни надзор комуникација и прикупљање података о личности, неретко, немају никакву правну основу, већ се спроводе произвољно од стране обавештајних агенција широм света. На овом месту ће акценат бити стављен на праксу Европског суда за људска права, који је испитивао усклађеност поступака јавне власти са чланом 8. Европске конвенције о људским правима.

Тако, један од случајева у којима је Европски суд за људска права заузео негативан став је поменути случај *Liberty and Others v. the United Kingdom* из 2008. године, где су две британске и ирске цивилне

невладине организације навеле да су између 1990. и 1997. године њихове телефонске везе, факсимили, као и електронске комуникације били пресретани од стране посебног тела Министарства одбране Велике Британије. У овом случају, Суд је сматрао да овакви поступци нису у складу са Конвенцијом, јер домаћи закон у релевантно време није довољно јасно указао, како би обезбедио адекватну заштиту од злоупотребе овлашћења, обим или начин вршења веома широке дискреционе моћи која је дата држави да пресреће и испитује спољне комуникације. Конкретно, није изнео у форми доступном јавности било какву назнаку процедуре коју треба следити за испитивање, дељење, чување и уништавање пресретнутог материјала (European Court of Human Rights 2022).

Суд се негативно изјаснио и у случају *Szabó and Vissy v. Hungary* из 2016. године у погледу мађарских прописа о антитерористичком тајном надзору из 2011. године, где су апликанти тврдили да би били изложени непропорционалним и неоправданим мерама спровођеним из безбедносних разлога, потом у случају *Big Brother Watch and Others v. United Kingdom* из 2021. године, по основу жалбе новинара и организација за заштиту људских права, у погледу масовног пресретања комуникација и прибављања података од стране провајдера електронских услуга, као и у случају *Ekimdzihiev and Others v. Bulgaria* из 2022. године, с обзиром на мањкавости постојеће бугарске легислативе у погледу тајног надзора (European Court of Human Rights 2022).

Било је и одлука у којима је Европски суд за људска права заузео став да није дошло до кршења члана 8. Конвенције. Такве одлуке заузете су, на пример, у случају *Klass and Others v. Germany*, где је утврђено да је немачка легислатива која је омогућила сајбер надзор била оправдана у интересу националне безбедности, или у случају *Kennedy v. The United Kingdom* из 2010. године, где је Суд закључио да је британско законодавство јасно прописало процедуре за одобравање и обраду налога за пресретање, као и обраду, саопштавање и уништавање прикупљених података (European Court of Human Rights 2022).

С обзиром на случај Едварда Сноудена, све већу забринутост јавности за очување права на приватност, као и надолазећа времена сајбер ратова, за очекивати је да ће у наредном периоду бити све више негативних одлука институција ЕУ, као и међународних тела широм света.

ЗАКЉУЧАК

Анализа праксе Европског суда за људска права и релевантних аката УН показала је да се очувању права на приватност поступа са великом пажњом. Показало се да сајбер надзор, односно сајбер шпијунажа представља прави изазов за право на приватност, стога је потребно јасно прецизирати услове под којима се право на приватност може ограничити. С тим у вези, ограничење права на приватност могуће је уколико је прописано легислативом која је транспарентна и доступна грађанима, при чему прописи морају бити таквог карактера да је могуће предвидети ефекте њихове примене. Даље, право на приватност се може ограничити само уколико је то пропорционално са обимом ограничења права на приватност и ако постоји легитимни циљ за тако нешто, као што је очување националне безбедности, јавног здравља, економских интереса државе и слично.

Без обзира на изузетке предвиђене Европском конвенцијом о заштити људских права и основних слобода, остаје дилема да ли ће акти масовног (сајбер) надзора, односно сајбер шпијунаже бити оправдани. То ће зависити од законодавства дате државе којом је уређено спровођење надзора од стране обавештајних служби и евентуалних ограничења која су прописана. С тим у вези, пракса Европског суда за људска права поставила је одређене стандарде. Најпре, законодавством се мора прецизно прописати под којим условима обавештајне агенције могу предузимати акте масовног (сајбер) надзора према појединцима. Потом, морају се формирати независна тела која би могла да врше контролу над спровођењем операција масовног надзора и њихове усклађености са правним стандардима заштите права на приватност. Најзад, спровођење мера (сајбер) надзора мора бити у складу са легитимним циљевима и пропорционално, то јест уколико се утврди да се легитимни циљ могао остварити мерама или средствима која су мање рестриктивна у односу на ограничење људских права, тада ће се радити о незаконитој делатности. Међутим, остаје проблем у случајевима када се мерама надзора дође до информација о трећим невиним лицима лицима и тако наруше њихова људска права. Случај Едварда Сноудена и обелодањене злоупотребе од стране NSA захтеваће у будућности много труда на унапређењу важеће правне регулативе широм света.

ЛИТЕРАТУРА

Бошковић, Мило. 2017. *Лексикон безбедности.* Београд-Нови Сад: Службени гласник.

Домазет, Синиша и Славица Динић. 2022. „Међународноправни аспекти масовног надзора и импликације на приватност.“ *Култура полиса 19* (1): 79-97.

Јовановић, Светлана. 2014. “Приватност и заштита података на интернету”. Твининг пројекат ЕУ – зборник „Везе cyber криминала са ирегуларном миграцијом и трговином људима”, Београд: Министарство унутрашњих послова Републике Србије.

Кригер, Волфганг. 2016. *Историја тајних служби: од фараона до НСА.* Београд: Лагуна.

Тепавац, Дејан. 2019. „Шпијунажа као облик угрожавања пословних информација.“ *Војно дело* 71(3): 164. doi: 10.5937/vojdelo1903163T

Androulidakis Iosif , Fragkiskos – Emmanouil Kioupakis. 2016. *Industrial Espionage and Technical Surveillance Counter Measurers.* Switzerland: Springer

Boban, Marija. 2012. The right to privacy and the right to access information in the modern information society. *Collected papers of the Law Faculty of the University of Split,* 49(3): 581-582.

Case Klass ond Others v. Germany. No. 5029/71 Judgment of the European Court of Human Rights (Plenary) on Merits and Just satisfaction of 06 September 1978, ECLI:CE:ECHR:1978:0906JUD000502971

Case of Liberty and Others v. the United Kingdom, No. 58243/00, Judgment of the European Court of Human Rights (First Section) on Merits and Just satisfaction of 01 July 2008, ECLI:CE:ECHR:2008:0701JUD005824300

Case Mikulić v. Croatia, No. 53176/99 Judgment of the European Court of Human Rights (First Section) on Merits and Just satisfaction of 7 February 2002, ECLI:CE:ECHR:2002:0207JUD005317699

Case Pretty v. United Kingdom Judgment. No. 2346/02 Judgment of the European Court of Human Rights (Fourth Section) on Merits and Just satisfaction of 29 April 2002, ECLI:CE:ECHR:2002:0429JUD000234602

Case of Szabo and Vissy v. Hungary, No. 37138/14, Judgment of the European Court of Human Rights (Fourth Section) on Merits and Just satisfaction of 14 March 2016, ECLI:CE:ECHR:2016:0112JUD003713814

Case Roman Zakharov v. Russia, No. 47143/06, Judgment of the European Court of Human Rights (Grand Chamber) on Merits and Just satisfaction of 04 December 2015, ECLI:CE:ECHR:2015:1204JUD004714306

Case Shimovolos v. Russia, No. 30194/09, Judgment of the European Court of Human Rights (First Section) on Merits and Just satisfaction of 21 June 2011, ECLI:CE:ECHR:2011:0621JUD003019409

Case Szabo v. Hungary, No. 37138/14, Judgment of the European Court of Human Rights (Fourth Section) on Merits and Just satisfaction of 12 January 2016, ECLI:CE:ECHR:2016:0112JUD003713814

Case Weber and Saravia v. Germany, No. 54934/00 Judgment of the European Court of Human Rights (Third Section) on Merits and Just satisfaction of 29 June 2006, ECLI:CE:ECHR:2006:0629DEC005493400

Cho, Hichang., Rivera-Sanchez, Milagros., Sun Sun, Lim. 2009. A Multinational Study on Online Privacy: Global Concern and Local Responses. *New Media & Society,* 11(3): 395-416. doi: HYPERLINK "http://dx.doi.org/10.1177/1461444808101618" \t "_blank" 10.1177/1461444808101618

Coleman, Kevin. 2008. „The Growing Risk of Cyber Attacks and other Security Threats (the Risk Report)." Last accessed January 22, 2022. https://www.hwphillips.com/wp-content/uploads/2012/09/The-Growing-Risk-of-Cyber-Attack-and-Other-Security-Threats.pdf.

Cyberspace Administration of China. 2016. "China Copyright and Media." Ed. Rogier Creemers. Cyberspace Administration of China. 26 December. Last accessed January 21, 2022. https://chinacopyrightandmedia.wordpress.com/2016/12/27/national-cyberspace-security-strategy/.

Demarest, Geoffrey. 1996. „Espionage in International LAw." *Denver Journal of International Law and Policy* 24 (2): 321, 325-326.

European Court of Human Rights. 2022. "Mass surveillance". *European Court of Human Rights* Strasbourgh, January. Last accessed March 23, 2022. https://www.echr.coe.int/documents/fs_mass_surveillance_eng.pdf.

Goldman, Zachary, and Damon McCoy. 2016. „Economic Espionage: Deterring Financially Motivated Cybercrime." *Journal of National Security Law and Policy* 8(3): 595, 597. Last accessed January 14, 2022. https://jnslp.com/wp-content/uploads/2017/10/Deterring-Financially-Motivated-Cybercrime_2.pdf.

Human Rights Committee. 1999. "General Comment No. 27: Article 12 (Freedom of Movement)". *Human Rights Committee*, November 2 1999. https://www.refworld.org/pdfid/45139c394.pdf

International Groups of Experts. 2017. "Tallinn manual 2.0 on the international law applicable to cyber operations". Last accessed 15. March 2022. https://assets.cambridge.org/97811071/77222/frontmatter/9781107177222_frontmatter.pdf

International Covenant on Civil and Political Rights [ICCPR], 16 December 1966, UNTS 14668

Internet World Stats. 2021. "World Internet Users and 2021 Population Stats". 3 July. Last accessed January 14, 2022. https://www.internetworldstats.com/stats.htm.

Kilovaty, Ido. 2016. „World Wide Web of Exploitations – The Case of Peacetime Cyber Espionage Operations Under International Law: Towards a Contextual Approach." *The Columbia Science and Technology Law Review* 18(1):47. Last accessed January 20, 2022. https://doi.org/10.7916/stlr.v18i1.4012

Lin, Herbert. 2010. „Offensive Cyber Operations and the Use of Force." *Journal of National Security, Law and Policy* 4(1):63. https://jnslp.com/wp-content/uploads/2010/08/06_Lin.pdf .

Office of the High Commissioner for Human Rights. 1988. "CCPR General Comment No. 16: Article 17 (Right to Privacy) The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour of Reputation". New York, 08 April. Last accessed March 06, 2022. file:///D:/DOWNLOADS/453883f922.pdf.

President of the United States. 2012. „Presidental Policy Directive/PPD-20." *US Cyber Operations Policy.* USA, October. Last accessed January 21, 2022. https://irp.fas.org/offdocs/ppd/ppd-20.pdf.

UK HM Government. 2016. „Government of the U.K." *National Cyber Security Strategy 2016 to 2021.* 1 November. Last accessed January 21, 2022. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf.

United Nations General Assembly. 2013. "The right to privacy in the digital age". New York, 20 November. Last accessed March 06, 2022. file:///D:/DOWNLOADS/A_C-3_68_L-45_Rev-1-EN.pdf.

United Nations General Assembly. 2015. "The right to privacy in the digital age: resolution". United Nations. Last accessed December 29, 2020 from file:///C:/Users/S&B/AppData/Local/Temp/A_RES_69_166-EN.pdf

United Nations General Assembly. 2016. "The right to privacy in the digital age". United Nations General Assembly. New York, 16 November. Last accessed March 20, 2022. https://tind-customer-undl.s3.amazonaws.com/0ec406a1-7841-48f0-8b10-0992e162549a?response-content-disposition=attachment%3B%20filename%2A%3DUTF-8%27%27A_C-3_71_L-39_Rev-1-EN.pdf&response-content-type=application%2Fpdf&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Am.

United Nations General Assembly. 2014. "The Right to privacy in the Digital Age". United Nations General Assembly. New York, 30 June. Last accessed March 19, 2022. https://documents-dds ny.un.org/doc/UNDOC/GEN/G14/088/54/PDF/G1408854.pdf?OpenElement.

Siniša Domazet

Faculty of security studies, Educons University, Sremska Kamenica

CYBER ESPIONAGE AND THE RIGHT TO PRIVACY FROM THE ASPECT OF THE PREVIOUS PRACTICE OF THE EUROPEAN COURT OF HUMAN RIGHTS AND THE UNITED NATIONS

Resume

Cyber espionage in the 21st century is a challenge in international relations, as well as its connection to human rights, primarily the right to privacy. The subject of the research is the analysis of the mutual relationship between the activities of modern intelligence services and their efforts to protect national security on the one hand and the need to protect the right to privacy on the other hand. It has been established that the right to privacy may be restricted under certain circumstances. Acts of the United Nations and the jurisprudence of the European Court of Human Rights have defined appropriate standards in assessing the legality of restrictions on the right to privacy. The research showed that the disputed measure must have a basis in domestic law. Further, the law should be accessible to a given person, who must be able to foresee its consequences for him. It must also be ensured that covert surveillance measures are applied only when they are necessary in a democratic society, in particular by providing adequate and effective safeguards and guarantees against abuse. In any case, it is necessary to weigh the proportionality of the supervision measure with the scope of the restriction of the right to privacy, as well as that there is a legitimate goal for such a thing. The normative method and legal-logical methods of induction and deduction were used in the research.

Keywords*:* Law, Security, Cyberspace, Mass Surveillance, Intelligence Services