British Embassy Podgorica

THE AIRE CENTRE
Advice on Individual Rights in Europe

OPEN SOCIETY FOUNDATIONS

CEDEM
CENTRE FOR DEMOCRACY AND HUMAN RIGHTS

PRAVO NA PRIVATNOST U CRNOGORSKOM ZAKONODAVSTVU I EVROPSKOJ PRAKSI

British Embassy Podgorica

THE AIRE CENTRE
Advice on Individual Rights in Europe

OPEN SOCIETY FOUNDATIONS

CEDEM
CENTRE FOR DEMOCRACY AND HUMAN RIGHTS

PRAVO NA PRIVATNOST U CRNOGORSKOM ZAKONODAVSTVU I EVROPSKOJ PRAKSI

Mart 2012.

Centar za demokratiju i ljudska prava (CEDEM), Podgorica
www.cedem.me

AIRE CENTAR, London
www.airecentre.org

Ovaj tekst je pripremljen uz podršku Britanske ambasade u Podgorici i Fondacija za otvoreno društvo, kroz Think Tank Fond. Mišljenja iznijeta u ovom tekstu predstavljaju isključivu odgovornost Centra za demokratiju i ljudska prava (CEDEM) i AIRE Centra, i ni na koji način ne odražavaju stavove Britanske ambasade u Podgorici i Fondacija za otvoreno društvo.

NAZIV PUBLIKACIJE:

PRAVO NA PRIVATNOST U CRNOGORSKOM ZAKONODAVSTVU I EVROPSKOJ PRAKSI

IZDAVAČ:

Centar za demokratiju i ljudska prava - CEDEM
Bulevar Džordža Vašingtona 51/3, Podgorica
+382 20 234 114; +382 20 234 368
info@cedem.me

ZA IZDAVAČA:

Mr Nenad Koprivica

ŠTAMPA:

Studio Mouse

TIRAŽ: 100

PRAVO NA PRIVATNOST U CRNOGORSKOM ZAKONODAVSTVU I EVROPSKOJ PRAKSI, SA FOKUSOM NA TAJNOST PISAMA I DRUGIH SREDSTAVA OPŠTENJA I ZAŠTITU LIČNIH PODATAKA

Uvod

Ovaj tekst je inicijativa Centra za demokratiju i ljudska prava (CEDEM) i AIRE Centra iz Londona, koja je nastala sa ciljem da se, kroz formu predloga praktičnih politika, pokuša uticati na promjenu stanja u oblasti koja se čini važnom za svako demokratsko društvo, sa aspekta poštovanja osnovnih ljudskih prava i sloboda, a samim tim i vladavine prava. Ovim tekstom se prije svega želi ukazati na moguća kršenja prava na privatnost kroz praksu i sprovođenje zakona, i pokrenuti inicijativa za izmjenu zakonodavstva, promjenu prakse, tumačenje Ustava i zakona i, samim tim, stvaranje ambijenta za puno poštovanje ovog ljudskog prava i povećanje povjerenja građana u vladavinu prava u Crnoj Gori. Tekst sadrži ekspertski izvještaj o zakonodavnom okviru prava na privatnosti i zaštite podataka u Crnoj Gori, kao i pregled Evropske konvencije o ljudskim pravima i evropskog prava, o pitanjima koja se odnose na zaštitu prava na privatnost.

Ova inicijativa je utemeljena na pretpostavci da organi državne vlasti i druge institucije, sprovodeći zakone i postupajući u konkretnim slučajevima, rade to u uvjerenju da se na taj način, u potpunosti, poštuju zakoni i međunarodni sporazumi, potpisani i ratifikovani od strane Crne Gore, te da je njihovo postupanje u skladu sa Ustavom. Polazeći od ove pretpostavke, namjera je autora da takav stav provjeri pred laičkom i profesionalnom javnošću, i da tako pokrene na akciju sve nadležne institucije, koje bi se, u bilo kom dijelu ovog pitanja, mogle osjetiti prozvane da svojim doprinosom pomognu iznalaženju pravnog rješenja, bez ikakvih dilema.

Potreba za definisanjem pojma privatnosti

U različitim kulturama postoje različite ideje o nivou potrebe za zaštitu prava na privatnost, na koje pojedinci imaju pravo, i u kojim kontekstima.

Jednostavnu modernu definiciju prava na privatnost dao je u 19.vijeku Američki sudija Cooley, koji je definisao ovo pravo kao "pravo da se bude sam" "the right to be let alone". Ova definicija spada u negativnu formulaciju ovog prava.

Sudija Brandeis je 1928. godine o ovom pitanju pisao sljedeću definiciju prava na privatnost u svom, kasnije široko citiranom mišljenju (u predmetu Olmstead protiv SAD 438, 478, 1928): *„Tvorci našeg Ustava su preuzeli odgovornost da obezbijede uslove koji su povoljni u težnji za srećom (...)Oni su dali, kao protiv vlasti, pravo da budemo ostavljeni na miru – najopsežnije od svih prava i pravo koje najviše cijene civilizovani ljudi"*. Na ovaj način je pravo na privatnost, koje se izričito ne pominje u Ustavu SAD, postepeno postalo osnovni strukturni element Ustava. Pred Vrhovnim sudom SAD i dan danas se, iznova, vodi bitka o primjeni prava na privatnost.

Sljedeću, isto tako jednostavnu definiciju, dao je Geoffrey Robertson 1993.godine kada je predložio da se pravo na privatnost definiše "pravo pojedinca da mu bude omogućeno da dio svog života provede iza vrata na kojima je napisano "ne uznemiravaj" - the right to be able to live some part of life behind a door marked 'do not disturb"...

Savremeni koncept prava na privatnost stavlja naglasak na tzv. kontrolu informacija od strane građanina. To znači da pojedinac ili grupa, u skladu sa svojim željama, saopštavaju informacije o sebi i kontrolišu tačnost informacija u zbirkama podataka koje su prikupljene na pravno dozvoljen, kao i nedozvoljen način.
Osim onih, zakonom propisanih slučajeva, kada se lične informacije moraju dati onima koji ih prikupljaju i obrađuju, u ostalim slučajevima, pojedinac ili grupa sami određuju koje će informacije dati, kome će ih dati i kako će ih saopštiti. U slučajevima kada se informacije i podaci obavezno prikupljaju na osnovu zakona, i onda mora postojati obaveza, za onog ko ih prikuplja i obrađuje, da ih čuva, prosljeđuje u zakonom propisane svrhe i kroz zakonom propisan postupak.

U savremenim pravnim teorijama, pravo na privatnost posmatra ličnost, to jest građanina kao centar prava, odnosno subjekta koji u svakom trenutku mora da zna ko, što i kako zna o njemu, i da u svakom trenutku ima pred sobom mehanizam za ispravljanje greške u vezi podataka koji se o njemu generiraju, te da ima sudsku zaštitu u slučaju nezakonite odrade i prikupljanja podataka.

Iz širokog spektra oblasti koji pokriva pravo na privatnost, u ovom radu ćemo se samo baviti jednim užim dijelom, koji se bavi privatnošću u dijelu telekomuniaicija, sa posebnim fokusom na telekominikacioni saobraćaj. Iako se radi o uskoj oblasti iz prava na privatnost, ona, po značaju za integritet ličnosti, često dolazi u prvi plan, izaziva pažnju, kontroverzu i zabrinutost kako zaštiti privatnost, bez koje se ne može govoriti o integritetu ličnosti. Zbog uloge telekominikacionog saobrajaća u vrijeme vrtoglavog tehničkog razvoja mobilne telefonije, osim dobrobiti koju donosi taj razvoj, u isto vrijeme se povećavaju i mogućnosti kršenja prava na privatnost. Ova kršenja, po težini i posljedicama koje mogu ostaviti na lični integritet pojedinaca, iziskuju efikasan odgovor države i društva koje pretenduje da bude demokratsko, i da poštuje ljudska prava i slobode.

Garancije prava na privatnost u crnogorskim ustavima

Prvi Ustav u istoriji Crne Gore je onaj Knjaževine iz 1905. Ovaj Ustav, koji nazivamo i oktroisani, jer ga je Knjaz Nikola, gospodar Crne Gore podario Crnogorcima, u članu 211 kaže: Nepovrediva je tajna pisama i telegrafskih depeša osim u slučaju rata i u slučaju krivične istrage.

Period Socijalističkog uređenja ustavotvorno započinje Ustavom Federativne Narodne Republike Jugoslavije 1946.godine. Ustav iz 1946. u članu 30 garantuje nepovredivost i tajnost pisama drugih sredstava opštenja, osim u slučaju krivične istrage, mobilizacije i ratnog stanja.

Jugoslovenski Ustav iz 1963. u članu 53 kaže: Tajna pisama i drugih sredstava opštenja je nepovrediva; samo Saveznim zakonom može se propisati da na osnovu odluke nadležnog organa može odstupiti od načela nepovredivosti tajne pisama i drugih sredstava opštenja, ako je to potrebno za vođenje krivičnog postupka ili bezbjednosti zemlje.

Ustav SFRJ iz 1974. članom 185 takođe garantuje nepovredivost pisama i drugih sredstava opštenja i kaže da se samo na osnovu odluke nadležnog organa može odstupiti od načela nepovredivosti

tajne pisama i drugih sredstava opštenja, ako je to potrebno za vođenje krivičnog postupka ili bezbjednosti zemlje.

Ustav Savezne Republike Jugoslavije iz 1992 godine, koji je ujedno i prvi Ustav nakon sloma socijalističkog političkog uređenja, garantuje pravo na privatnost, ali i prvi put Ustavom se garantuje zaštita ličnih podataka. Član 32 kaže: "Tajna pisama i drugih sredstava opštenja je nepovrediva. Saveznim zakonom se može propisati da se na osnovu odluke suda može odstupiti od načela nepovredivosti tajne pisama i drugih sredstava opštenja, ako je to neophodno za vođenje krivičnog postupka ili za odbranu Savezne Republike Jugoslavije."

Članom 33 istog Ustava se jamči zaštita podataka o ličnosti. Takođe se kaže da je upotreba podataka o ličnosti van namjene, za koju su prikupljeni, zabranjena. Nadalje se garanatuje svakome da bude upoznat sa prikupljenim podacima o ličnosti koji se odnose na njega, kao i pravo na sudsku zaštitu u slučaju zloupotrebe podataka o ličnosti. Uređenje ove oblasti se propisuje Saveznim zakonom.

Svi Ustavi, od prvog iz doba Knjaževine Crne Gore, preko onih Saveznih, u državama gdje je Crna Gora bila subjektivitet Federacije, prepoznavali su i garantovali pravo na privatnost, odnosno nepovredivosti pisama. U kvalitetu garancije su postojale razlike, posebno u dijelu gdje je državni organ imao ovlašćenje da odobri odstupanje od ovog prava.

Zakonom o zaštiti podataka o ličnosti iz 1998. godine je definisan način zaštite, ali je on sam bio najsporniji dio Zakona jer je propisivao da je Savezno Ministarstvo pravde organ koji se bavi nadzorom i zaštitom podataka o,ličnosti, što je bilo u direktnoj suprotnosti sa Direktivom 96/45, koja propisuje da se takva nadležnost mora povjeriti nezavisnom organu, a ne dijelu izvršne vlasti, koja bi, po prirodi fenomena, trebalo, na taj način, samu sebe da kontroliše. Osim ovog problema iz sadržaja Zakona, postojao je praktičan problem koji se ogledao u tome da ne postoje statistički dokazi da je Zakon uopšte primjenjivan, što svakako ne govori da su građani SRJ bili zadovoljni zaštitom ličnih podataka, nego prije da nijesu bili uopšte upoznati o svojim pravima, a i ako su bili upoznati, moguće je da nijesu vjerovali da se na ovaj način ona mogu efikasno štititi.

Kraj devedesetih, kada je usvojen ovaj zakon, se poklapa sa uvođenjem mobilne telefonije na prostoru tadašnje države Jugoslavije. Ova činjenica je važna jer se, u praktičnom smislu, po prvi put javlja mogućnost da se preplijetaju Ustavna prava na tajnost pisama, odnosno prepiske, sa pravom na zaštitu ličnih podataka, odnosno gdje je ta granica kada je u pitanju kršenje ovih prava, i kako se ona štite.

Zaštita prava na privatnost u dokumentima Savjeta Evrope i Evropske Unije

Zaštita prava na privatnost, na Evropskom nivou, ima solidan pravni okvir. Članom 8 Pravo na poštovanje privatnog i porodičnog života Evropske konvencije o osnovnim ljudskim pravima i slobodama i članom 7 Povelje o osnovnim ljudskim pravima Evropske unije. Premda je Crna Gora ratifikovala Evropsku konvenciju 2004. godine kao dio Državne zajednice Srbija i Crna Gora, to znači da je ona, od tada, i dio crnogorskog pravnog poretka u hijerarhiji prava iznad zakona, a niže od Ustava. Takođe su i presude Evropskog suda za ljudska prava u Strazburu, na isti način, dio crnogorskog pravnog poretka u skladu sa članom 9 Ustava Crne Gore iz 2007. godine.

Konvencija za zaštitu ličnosti, u vezi automatske obrade ličnih podataka, Savjeta Evrope iz 1981. je ratifikovana od strane Crne Gore 2005.

Direktiva Evropske Unije 95/46/EC iz 1995. o zaštiti prava o ličnosti, u vezi obrade i prometa istih, je jedan od najvažnijih dokumenata koji reguliše zaštitu ovih prava u zemljama članicama EU. Ova Direktiva je bila i osnov prilikom pisanja crnogorskog Zakona o zaštiti podataka o ličnosti, i tom prilikom zakonopisac je pokušao da u crnogorski zakon unese sve standarde Direktive, kako bi se i na taj način približio evropskom pravnom okviru, a samim tim i praksi.

Direktiva Evropske Unije 2002/58/EC iz 2002. se bavi pravom na privatnost vezanom za elektronske komunikacije, odnosno, zadržavanje podataka tzv. zadržani podaci (retention data). Ona je osnov za Zakon o elektronskim komunikacijama, čak i za države koje su, kao Crna Gora, na putu prijema u EU, a ne samo za članice EU.

Na kraju, ne treba izgubiti iz vida ni Povelju o osnovnim pravima i slobodama, i posebno član 8.

Potpisivanjem i ratifikacijom Direktivama. Sporazum o stabilizaciji i pridruženju, Crna Gora se članom 81 istog, obavezala da, i prije nego što postane članica, poštuje i primjenjuje evropske standarde u pogledu zaštite ličnih podataka.

Definisanje problema

Crna Gora se, kao i druge demokratske države, suočava sa ozbiljnim bezbjedonosnim izazovima, kao što su borba protiv organizovanog kriminala i korupcije, koji mogu da zadiru u samu srž države, odnosno funkcionisanja vladavine prava i ekonomskog razvoja. Terorizam može, ubuduće, biti realna prijetnja, kao što je već više puta viđen problem savremenog svijeta. Borba protiv najtežih oblika kriminala mora biti beskompromisna i efikasna, ali u isto vrijeme, sa garancijama poštovanja osnovnih prava i sloboda.

Ovdje ćemo se baviti problemom vezanim za jedno od osnovnih prava, a to je pravo na privatnost, koje može biti ugroženo korišćenjem sredstava za borbu protiv najtežih oblika krivičnih djela.

Pitanje ograničenja prava na privatnost u elektronskim komunikacijama, osim ustavnih garancija i međunarodnih dokumenata, uređuje i Zakonik o krivičnom postupku. U poglavlju 9. ZKP-a definisane su mjere tajnog nadzora. Član 157 tog poglavlja u stavu 1. kaže da se može odrediti tehničko snimanje telefonskih razgovora, odnosno, druge komunikacije koja se vrši putem sredstava za tehničku komunikaciju na daljinu.

Tehničko snimanje se može odrediti samo ako postoje osnovane sumnje da je neko lice samo, ili u saučesništvu sa drugim, izvršilo, vrši ili se priprema za vršenje krivičnih djela iz člana 158 ZKP. U ovom slučaju se kaže da se ove mjere sprovode ako se, na drugi način, ne mogu prikupiti dokazi ili bi njihovo prikupljanje zahtijevalo nesrazmjerni rizik ili ugrožavanje života ljudi.

Mjere tajnog nadzora su veoma poznate, korišćene u savremenim demokratskim društvima, i predstavljaju efikasan oblik tzv. specijalnih istražnih tehnika. Ove mjere se zakonski primjenjuju samo na ograničen krug krivičnih djela. Osnovna je pretpostavka da se mjere tajnog nadzora određuju, jer se drugim dokaznim sredstvima ne može postići cilj u borbi protiv kriminala. Ove mjere se koriste u izviđajnom dijelu krivičnog postupka.

Opravdanost mjera tajnog nadzora najviše uporišta ima u saznanjima da se priprema krivično

djelo iz člana 158. ZKP. Ovdje takođe treba ponoviti da se mjere preduzimaju samo ako se na drugi način ne bi mogli prikupiti dokazi, ili bi njihovo prikupljanje bilo skopčano sa nesrazmjernim rizikom, ili ugrožavanjem života ljudi.

Mjere tajnog nadzora tehničkog snimanja telefonskih razgovora može, na obrazloženi predlog državnog tužioca, odrediti sudija za istragu, pisanom naredbom. Za pitanje zaštite privatnosti je važno da su predlog i naredba za određivanje mjera sastavni dio krivičnog spisa, i treba da sadrže raspoložive podatke o licu prema kome se određuju, krivično djelo zbog kojeg se određuju, činjenica iz kojih proističe potreba njihovog preduzimanja, rok trajanja koji mora biti primjeren ostvarenju cilja mjere, način, obim i mjesto sprovođenja mjera.Sudija za istragu, uz naredbu za izvršenje ovih mjera, će izdati poseban nalog u kojem će navesti samo telefonski broj ili e–mail adresu i trajanje mjere, a nalog će policija predati telefonskim operaterima, u postupku izvršenja mjere. Operateri su dužni da policiji omoguće izvršenje ovih mjera, dok su sva službena lica, koja učestvuju u postupku donošenja naredbe i izvršenja mjera, dužna da, kao tajne podatke, čuvaju podatke koje su saznali u postupku.

Razgovori, koji se obavljaju putem fiksne telefonske linije ili pak putem mobilnog telefona, smatraju se telefonskim razgovorima, dok se razmjena „SMS“ poruka smatra telefonskom komunikacijom, iako se ne radi o razgovoru, kako to tumačimo na osnovu čula.

Iz navedenog se vidi da mjere tajnog nadzora precizno određuju način na koje se sprovode, u dijelu snimanja telefonskih komunikacija, uslove pod kojima se mogu odrediti, te trajanje i način uništenja ovako dobijenih podataka, koji su vezani za privatnost nekog lica. Mjere tajnog nadzora, kako smo ih predstavili, ne bi se reklo da su uzrokovale obimnija kršenja prava na privatnost, bar na osnovu dostupnih informacija koje je javnost mogla da sazna. Za razliku od njih, tumačenje i primjena člana 257 ZKP su pokrenule mnoga pitanja i kod stručne, ali i kod laičke javnosti

Pravni problem počinje tada kada se otvori pitanje da li su listinzi telefonskih poziva, listinzi sms poruka i drugi podaci vezani sa telekomunikacioni saobraćaj, kao što su informacije sa baznih stanica, dio privatnosti takvog karaktera da bi trebalo da imaju sudsku zaštitu, ili je dotadašnja praksa i tumačenje člana 257 Zakonika o krivičnom postupku pravno valjano postupanje, u skladu sa Ustavom Crne Gore, međunarodnim dokumentima potpisanim i ratifikovanim, te samom duhu Zakonika o krivičnom postupku, koji svojim odredbama treba da detaljnije garantuje ostvarivanje prava na privatnost kroz krivično pravni postupak.

Dosadašnja praksa dobijanja listing telefonskih poziva i listinga sms poruka, na osnovu člana 257, iziskuje potrebu komentara. Ovim članom se omogućuje policiji da samoinicijativno, ili po zahtjevu državnog tužioca, preduzme potrebne mjere da bi se pronašao učinilac krivičnog djela, da se otkriju tragovi, prikupe obavještenja itd.

ZKP propisuje da, u cilju ispunjenja dužnosti, policija može da zatraži od pružaoca usluga elektronskih komunikacija provjeru identičnosti telekomunikacijskih adresa, koje su u određenom vremenu uspostavile vezu**.**

Upravo ova ovlašćenja uzrokuju pravne nedoumice, da li je to, kako tvrde iz policije, pravo da se dobiju listinzi ili samo da se utvrdi telekomunikacijska adresa, što bi, prema mišljenju autora ovog teksta, se odnosilo na to ko je vlasnik telefona i broja.

Bilo kako bilo, ovaj član ZKP ne obavezuje policiju da za pribavljanje ovih podataka imaju naredbu suda. Međutim, ako se radi o tumačenju člana 257 da se mogu dobijati i listinzi, onda se tu radi o tome da je ovaj član, prema mišljenju autora, suprotan Ustavu, Evropskoj konvenciji o zaštiti ljudskih prava i sloboda, odnosno, članu 8 i praksi suda u Strazburu.

Ako bi ovo sporno pitanje razumjeli tako da policija u pretkrivičnom postupku zaista ima ovlašćenja da, u slučaju postojanja osnova sumnje da je krivično djelo izvršeno (djelo koje se goni po službenoj dužnosti), može od operatera zahtijevati dostavljanje listinga telefonskih poziva i sms poruka, kao i lokacije mobilnog telefona u trenutku ostvarenja komunikacije, onda se zaista ostavlja mogućnost za obimna kršenja prava na privatnost.

Prvo pitanje koje se nameće, uslijed nepreciznosti propisane procedure, što se dešava sa podacima prikupljenim na ovaj način, ako se protiv lica, čiji su podaci prikupljani, nikad ne pokrene krivični postupak. U tom slučaju, ta lica nikad ne bi saznala da su se podaci o njima obrađivali od treće strane, i samim tim ne bi mogla ostvariti pravo da to saznaju, kad prestanu potrebe za prikupljanje i obradu ovih podataka. Nadalje, ne zna se što se dešava sa ovim podacima, kako i koliko se čuvaju, te na koji se način uništavaju, jer se, po pravilima o zaštiti ličnih podataka, ovi podaci ne smiju trajno čuvati.

Zaštita podataka o ličnosti u evropskoj praksi

1. Član 8 i Evropska konvencija o ljudskim pravima (Konvencija)

Član 8(1) predviđa da svako ima pravo na poštovanje svog privatnog i porodičnog života, svog doma i prepiske. Član 8(2) predviđa da se javne vlasti neće miješati u vršenje ovog prava, osim ako to nije u skladu sa zakonom i neophodno u demokratskom društvu. Član 8 je, dakle, kvalifikovano pravo, i u procjeni da li je došlo do kršenja člana 8, mora se razmotriti da li: je bilo miješanja u vršenju ovog prava; je miješanje bilo u skladu sa zakonom; je miješanje bilo neophodno u demokratskom društvu; i da li je miješanje bilo proporcionalno legitimnim ciljevima kojima se težilo.

Takođe je važno primijetiti da član 8 Konvencije ne predviđa *pravo na privatnost*. Umjesto toga, zaštićeno je pravo pojedinca na privatni život i porodični život ili pravo na prepisku.

a. Zadržavanje ličnih podataka

Pitanja zadržavanja podataka se mogu pojaviti u kontekstu člana 8, u situacijama kada javni organi dobijaju i zadržavaju lične podatke, bez pristanka osoba koje su u pitanju. Kao što je gore već rečeno, da bi se našlo kršenje člana 8, neophodno je prvo naći miješanje u prava iz člana, a zatim procijeniti opravdanost tog miješanja.

Predmet *S i Marper protiv UK*[1] je predmet u kojem je jedan broj lica bio uhapšen, i kojima su uzeti uzorci ćelija, DNK i otisci prstiju. Ta lica su kasnije bila oslobođena, a policija je tražila da zadrži te podatke. Od Suda se tražilo da razmotri da li je zadržavanje podataka od strane organa vlasti bilo kršenje člana 8.

1 [2008].

Sud je, prvo, razmotrio da li bi zadržavanje uzoraka ćelija, DNK i otisaka prstiju[2] predstavljalo miješanje u prava podnosilaca predstavke iz člana 8. Razmatrajući to pitanje, Sud je smatrao da je došlo do miješanja u prava podnosioca predstavke iz člana 8 zbog: opsega ličnih podataka sadržanih u ćelijskim uzorcima; sposobnosti DNK da pruži sredstva za identifikovanje genetskih odnosa između osoba; i objektivno jedinstvenih podataka, sadržanih u otiscima prstiju, koji mogu uticati na privatni život osoba. Kada je Sud našao da je došlo do miješanja sa pravom iz člana 8, nastavio je da procjenjuje da li je to miješanje bilo opravdano.

Procjenjujući opravdanost miješanja u prava iz člana 8, Sud je u predmetu *S i Marper* smatrao da paušalna i nasumična priroda ovlašćenja za zadržavanje otisaka prstiju, ćelijskih uzoraka i DNL profila osoba, osumnjičenih ali ne i osuđenih za krivična djela, nije uspjela da pogodi pravu ravnotežu između konkurentnih javnih i privatnih interesa.

Dok je gornja kratka analiza korisna za shvatanje pristupa koji Evropski sudi zauzima prema ličnim podacima, važno pitanje je kako je Sud došao do svoje odluke; posebno, koji faktori su uzeti u obzir prilikom donošenja odluke. Kod utvrđivanja da li zadržavanje nekih vrsta podataka predstavlja kršenje člana 8, analiza *S i Marper* sugeriše da Sud prvo razmatra količinu informacija sadržanih u nekoj posebnoj vrsti podataka. U slučaju kada informacije mogu identifikovati posebne lične aspekte određene osobe, a te informacije se ne mogu smatrati neutralnim za identifikaciju, čini se da će postojati miješanje u prava iz člana 8.

U pogledu procjene opravdanosti miješanja, Sud vaga javne i privatne interese koji su u pitanju. U tom vaganju, Sud je iznio komentar da je potreba za garancijama (kako bi se spriječilo nekonzistentno postupanje u odnosu na član 8) veća u slučajevima kada lični podaci podliježu automatskoj obradi, ili kada se podaci koriste u policijske svrhe. Sud je, takođe, iznio primjedbu da bi domaće pravo trebalo osigurati da podaci, koji se čuvaju, budu relevantni, a ne pretjerani u odnosu na svrhu radi koje se isti čuvaju. Kao što je to uvijek slučaj sa vaganjem konkurentnih prava, razumijevanje tačnog procesa, koji sprovodi Evropski sud, može biti teško zato što se to radi sporadično, od slučaja do slučaja. Ono što, međutim, treba reći je da je analiza vezana za posebne činjenice, i da će, pored procjene prethodno pomenutih faktora, Sud posvetiti pažnju Direktivi Savjeta Evrope o zaštiti podataka.

b. Pristup zadržanim podacima

Pitanja koja se tiču pristupa podacima, zadržanim od strane organa vlasti, mogu se pojaviti kada se smatra da zadržani podaci spadaju pod opseg člana 8. Pristup zadržanim podacima se može postići, kako putem pozitivnih, tako i putem negativnih obaveza iz člana 8.

Gaskin protiv UK[3] je bio predmet u kome je jedna osoba pokušala dobiti pristup ličnim podacima, kako bi došla do odgovora na pitanja vezanih za svoje djetinjstvo. Njemu je, međutim, lokalni organ odbio davanje pristupa tim evidencijama. Podnosilac predstavke se žalio da, odbijanjem

2 U predmetu *McVeigh* prvo je ispitano pitanje uzimanja i zadržavanja otisaka prstiju kao jedna u nizu istražnih mjera. U ovom predmetu, bilo je prihvaćeno da su barem neke od mjera predstavljale miješanje u privatni život podnosioca predstavke, ostavljajući otvorenim pitanje da li bi samo zadržavanje otisaka prstiju dovelo do takvog miješanja.

3 [1989].

davanja pristupa evidencijama vezanim za njegovo djetinjstvo, lokalni organ nije ispunio svoje pozitivne obaveze iz člana 8. Evropski sud je prvo smatrao da se evidencije, kojima je gospodin Gaskin tražio pristup, odnose na njegov privatni život, i da je nemogućnost pristupa ovim informacijama aktivirala član 8. Razmatrajući opseg pozitivnih obaveza iz člana 8, Sud je smatrao da član 8 zahtijeva da svako treba imati mogućnost da ustanovi detalje o svom identitetu, kao pojedinačnom ljudskom biću i da, u načelu, organi vlasti ne bi trebalo u tome da ih ometaju. Utvrđujući da li su ispoštovane pozitivne obaveze iz člana 8, Evropski sud je smatrao da treba uzeti u obzir "pravičnu ravnotežu… između opšteg interesa zajednice i interesa pojedinca … Ciljevi pomenuti u 8(2) mogu biti relevantni za postizanje te ravnoteže."[4] U predmetu *Gaskin* Sud je, konačno, smatrao da organ vlasti nije ispoštovao svoje pozitivne obaveze.

Predmet *Segerstedt-Wiberg i ostali protiv Švedske* je jedan drugi predmet koji se tiče pristupa zadržanim podacima. Za razliku od predmeta *Gaskin,* međutim, u predmetu *Segerstedt-Wiberg* razmatra se pristup zadržanim podacima kroz negativne obaveze iz člana 8. Tri podnosioca predstavke su tražila pristup policijskim evidencijama koje sadrže informacije o njima. Međutim, nacionalni organi su odbili da odobre pristup kompletnim evidencijama, uz tvrdnje da bi kompletno objelodanjivanje moglo ugroziti buduće operacije nadzora. U postupku pred Evropskim sudom, podnosioci predstavke su se žalili da je odbijanje vlasti, da otkrije opseg informacija koje se čuvaju o njima, činilo kršenje njihovih prava iz člana 8. Evropski sud je smatrao da nije bilo kršenja člana 8, a dolazeći do svoje odluke, rezonovao je da, iako su se vlasti miješale u prava garantovana članom 8 odbijanjem pristupa podnosiocima predstavke, odbijanje potpunog pristupa evidenciji nacionalne tajne policije je bilo neophodno u datim okolnostima, budući da Država može imati legitimnu bojazan da bi davanje takvih informacija moglo ugroziti efikasnost sistema tajnog nadzora, namijenjenog zaštiti nacionalne sigurnosti.

Iz ovih predmeta je važno primijetiti da pojedinac može pokušati da dobije pristup zadržanim podacima, bilo preko pozitivnih ili negativnih obaveza, sadržanih u članu 8. Na osnovu predmeta *Gaskin*, pozitivna obaveza se može tumačiti kao veoma široka. Važno je, međutim, primijetiti da, kao što je Evropski sud pojasnio u predmetu *Gaskin*, član 8 ne dodjeljuje opšte pravo pristupa zadržanim informacijama.

c. Nadzor

Operacije nadzora, od strane nacionalnih organa, su važan dio osiguranja krivičnog progona, a time i sigurnosti nacije. Evropski sud za ljudska prava smatra nadzor osnovnim elementom policijskih istraga, a akcenat analize, u predmetima vezanim za nadzor, je, dakle, često na opravdanosti ili proporcionalnosti mjera nadzora.
Klass protiv Njemačke[5] je predmet u kojem je pet njemačkih advokata tvrdilo da je njemačko zakonodavstvo, dozvolivši državnim organima da prisluškuju telefonske razgovore, kako bi se zaštitili od neposrednih opasnosti, koje prijete slobodnom demokratskom ustavnom poretku države, prekršilo član 8. U predmetu *Klass* Sud je, prvo, utvrdio da je presretanje telefonskih razgovora predstavljalo miješanje u prava pojedinaca iz člana 8. U nizu predmeta poslije *Klass-a*, Sud je takođe potvrdio ovaj pristup.[6]

4 Stav 42 iz predmeta *Gaskin protiv UK.*
5 [1978].
6 *Malone protiv UK* podržava ovakav stav, a *PF i JH protiv UK* i *Halford protiv UK* predstavljaju mjerodavni za stav da presretanje telefonskih poziva u privatnom domu i na radnom mjestu predstavlja miješanje sa pravom iz

Evropski sud je, takođe, smatrao da tajni uređaji za prisluškivanje, postavljeni u kući podnosioca predstavke[7] i u policijskoj stanici[8], predstavljaju miješanje u prava pojedinca iz člana 8, kao i tajno video snimanje osobe u policijskoj ćeliji.[9]

Prilikom razmatranja opravdanosti miješanja u predmetima o nadzoru, Evropski sud je striktno primijenio zahtjev da mjere nadzora moraju biti u skladu sa zakonom. *Malone* je bio predmet protiv Ujedinjenog Kraljevstva, u kojem su organi vlasti prisluškivali telefonske razgovore gospodina Malone-a. Gospodin Malone se žalio da su, prisluškivanjem njegovih telefonskih razgovora, organi vlasti prekršili njegova prava iz člana 8. Evropski sud je smatrao da mjere, koje su preduzeli nacionalni organi, nisu bile u skladu sa zakonom, zato što se nije moglo reći, sa razumnom sigurnošću, koji elementi ovlašćenja za presretanje su bili inkorporirani u zakonska pravila, a koji elementi su ostali u domenu slobode odlučivanja izvršne vlasti. Do istog rezultata se došlo u predmetu *Khan protiv UK*[10], predmetu u kojem je prislušni uređaj bio tajno postavljen u kući podnosioca predstavke, a dobijeni dokazi su bili upotrijebljeni protiv njega na suđenju. U predmetu *Khan,* Sud je smatrao da nije postojala zakonska shema koja bi regulisala korišćenje prikrivenih uređaja za prisluškivanje. Smjernice koje su vlasti koristile, u vrijeme koje je u pitanju, nisu bile ni zakonski obavezujuće, niti direktno dostupne javnosti.

U predmetu *PG i JH protiv UK*[11], Sud je iskoristio priliku da razmotri da li su mjere tajnog nadzora bile neophodne u demokratskom društvu, i proporcionalne legitimnim ciljevima kojima se težilo. U ovom predmetu, podnosioci predstavke su tajno snimani u svom domu i u policijskoj ćeliji, nakon što je policija dobila dojavu da su namjeravali da počine provalnu krađu. Podnosioci predstavke su se žalili da je, u datim okolnostima, korišćenje prikrivenih uređaja za prisluškivanje, od strane policije, predstavljalo kršenje njihovih prava iz člana 8. Evropski sud je, međutim, smatrao da su mjere bile opravdane, zato što su informacije dobijene i korišćene u kontekstu jedne istrage u vezi sa suđenjem, zbog sumnje na kovanje zavjere radi počinjenja oružane pljačke. U ovom predmetu nije bilo identifikovano nijedno pitanje vezano za proporcionalnost.

Potrebno je, takođe, primijetiti da je u predmetu *Klass* Sud dalje razmatrao da li je miješanje u prava iz člana 8 bilo neophodno u demokratskom društvu i proporcionalno legitimnim ciljevima, kojima se težilo, nalazeći da su mjere bile neophodne u cilju sprječavanja nereda ili krivičnog djela.

U vezi sa nalaženjem miješanja u prava iz člana 8 u predmetima nadzora, iz analiziranih predmeta čini se da će, u većini slučajeva, tajni nadzor predstavljati miješanje u prava iz člana. To je tako, čak i u slučaju kada je lice izvan svog privatnog boravišnog prostora. U predmetu *Perry protiv UK*[12], predmetu gdje je policija trajno snimala podnosioca predstavke prilikom boravka u policijskom pritvoru, nakon što je u više navrata odbio da učestvuje u redu za identifikaciju, Sud je zaključio da pojedinac ima zonu interakcije sa ostalima, čak i u javnom kontekstu, koja može potpasti pod opseg privatnog života. Utvrđujući da li se mjere tajnog nadzora miješaju sa pravom nekog lica

člana 8, te da informacije, koje se odnose na telefonske brojeve koje je neko lice pozivalo, takođe potpadaju pod opseg člana 8.

7 *Khan protiv UK,*(2001) 31 EHRR.

8 *PG i JH* protiv *UK* i *Allan* protiv *UK.*

9 *Perry protiv UK* (17. jul 2003. godine).

10 [2001].

11 [1998].

12 17. jul 2003. godine

iz člana 8, Sud je, čini se, takođe, uzeo u obzir stalnost zadržanih podataka: u predmetu *Allan protiv UK*[13] gdje je policija tajno snimala razgovore podnosioca predstavke sa osobom sa kojom je dijelio ćeliju, Sud je smatrao da pitanja, vezana za privatni život, dolaze u prvi plan onda kada se pojave bilo kakve sistematske ili permanentne evidencije iz javnog domena.

Što se tiče procjene Suda o opravdanosti miješanja, „u skladu sa zakonom", zahtijeva jasno zakonsko pravilo, koje odobrava miješanje. Smjernice vlade neće biti dovoljne. Prilikom procjene da li je nadzor opravdan, iz analiziranih predmeta se čini da Sud izražava saosjećanje prema neophodnosti za uvođenje mjera tajnog nadzora. Artikulisanje faktora na koje je potrebno obratiti pažnju, prilikom razmatranja načina na koji se može uspostaviti ravnoteža u budućim predmetima, je, međutim, veoma teško.

d. Odnos između člana 8 i člana 6

Prilikom razmatranja predmeta, vezanih za član 8 unutar konteksta krivičnog pravosuđa, takođe je neophodno shvatiti odnos između pronalaženja kršenja člana 8 i člana 6. U nekim okolnostima, kada dokaz, prikupljen od strane policije, krši član 8, on takođe krši i član 6. Na takve predmete se najbolje pozivati kao na predmete o kršenju konvencijskih prava iz člana 6. Prije razmatranja sudske prakse, vezane za predmete o kršenju konvencijskih prava iz člana 6, potrebno je primijetiti da je sudska praksa Konvencije komplikovana, ponekad nekonzistentna, i često nekoherentna.

Podsjetimo se da su u predmetu *Khan,* pored isticanja kršenja člana 8, podnosioci predstavke, takođe, dokazivali da je, prilikom korišćenja dokaza dobijenih kršenjem člana 8, došlo do kršenja njihovih prava iz člana 6. U predmetu *Khan* Sud je našao da nije bilo kršenja člana 6, a dolazeći do takve odluke je zaključio: da nije bila njegova uloga da utvrdi koji dokazi su prihvatljivi ili neprihvatljivi, već da utvrdi da li je postupak u cjelini bio pravičan. Izvodeći tu vježbu, Evropski sud se oslonio na činjenicu da su podnosioci predstavke osporavali dokaz na svim nivoima nacionalnih sudova; i da, iako je taj dokaz, u stvari, bio jedini dokaz protiv podnosioca predstavke, nije bilo opasnosti od toga da dokaz bude nepouzdan, i stoga bude u skladu sa članom 6, potreba za podupirućim dokazom je bila manja.

Kao što je već rečeno, predmeti o kršenju konvencijskih prava iz člana 6 su nevjerovatno komplikovani, a nije svrha ovog polaznog dokumenta da obezbijedi sveobuhvatnu analizu sudske prakse u ovoj oblasti; umjesto toga, svrha ovog dokumenta je da naglasi postojanje problema, i da da kratak uvod u praksu Evropskog suda. U tom smislu, *Khan* je odlična polazna tačka. Iz predmeta *Khan* je moguće izvući sljedeće tačke: procjena po osnovu člana 6 je holistička vježba; razmatraće se sposobnost pojedinca da osporava dokaze pred nacionalnim sudovima; a tamo gdje su dokazi jedinstveni ili odlučujući, razmatraće se pouzdanost tih dokaza, kako bi se došlo do odluke da li se, oslanjanjem na njih, krši član 6.

13 [1999].

2. Pravo Evropske unije

Direktiva 95/46/EC je glavno zakonodavstvo koje reguliše zaštitu ličnih podataka širom Evropske unije, sa Okvirnom odlukom 2008/997/2008, koja pruža smjernice o prenosu podataka u krivičnim istragama. Član 8 Povelje EU o osnovnim pravima, takođe pruža zaštitu za pojedince, u odnosu na korišćenje i čuvanje ličnih podataka, dok član 16 Ugovora o funkcionisanju EU, obezbjeđuje pravni osnov za pravila o zaštiti podataka za sve aktivnosti unutar opsega prava EU.

a. Direktiva 95/46/EC (Direktiva o zaštiti podataka)

i. Ciljevi i opseg Direktive o zaštiti podataka

Prema članu 1 Direktive o zaštiti podataka, ciljevi Direktive su: zaštita osnovnih prava i sloboda fizičkih lica, posebno njihovo pravo na privatnost u odnosu na obradu ličnih podataka; kao i da osigura da države članice ne ograničavaju, ni zabranjuju, slobodan protok ličnih podataka između država članica. Postoji određeni stepen antagonizma između ovih ciljeva, i potrebno je postići ravnotežu između zaštite prava pojedinaca i osiguranja slobodnog kretanja podataka prilikom tumačenja i primjene Direktive.

Prema članu 3 Direktive o zaštiti podataka, Direktiva se primjenjuje na obradu ličnih podataka u cijelosti ili djelimično završenoj automatskim putem, i na obradu podataka na neki drugi način, koja je sastavni dio sistema za arhiviranje, ili je namijenjena da bude sastavni dio sistema za arhiviranje. Prema članu 3, Direktiva se ne primjenjuje na obradu ličnih podataka od strane fizičkog lica, tokom čisto ličnih ili porodičnih aktivnosti, i tokom neke aktivnosti koja ne potpada pod opseg prava Zajednice. U tom smislu, opseg Direktive o zaštiti ličnih podataka se neće proširiti na pitanja državne sigurnosti, ili na aktivnosti države na polju krivičnog prava. Veoma je važno primijetiti da pitanja, vezana za državnu sigurnost i krivično pravo, nisu uključena u opseg ove direktive. Pravila, koja se tiču kontrole i korišćenja podataka u ovim oblastima, stoga su pitanja nacionalnog prava.

ii. Definicije i opšta opažanja

Član 2 Direktive o zaštiti podataka daje definicije termina koji se upotrebljavaju širom Direktive. U svrhu ovog polaznog dokumenta, *lični podaci* znače informacije vezane za neku identifikovanu osobu, ili osobu koja se može identifikovati; *subjekat podataka* znači osobu na koju se podaci odnose; i *Kontrolor podataka* znači osobu ili pravno lice koje kontroliše i obrađuje podatke.

Važno je primijetiti da Direktiva o zašiti podataka, budući da je direktiva, zahtijeva sprovođenje od strane nacionalnih vlada, i da nacionalno zakonodavstvo o zaštiti podataka, stoga, varira između država članica. U skladu sa evropskim pravom, međutim, ukoliko država članica ne sprovede Direktivu na pravi način, pojedinac može direktno sprovesti pravila sadržana u Direktivi, u skladu sa odlukom Evropskog suda pravde u predmetu *Pubblico Ministero protiv Tullio Ratt.*[14]

Takođe je važno primijetiti da je Direktiva o zaštiti podataka komplikovana, i kako bi se pravilno

14 1978

shvatila, sugeriše se da se čita u njenoj osnovnoj formi. Ovaj polazni dokument, međutim, daje samo pregled Direktive o zaštiti podataka.

iii. Zaštita subjekata podataka

U skladu sa ciljevima Direktive o zaštiti podataka, lične podatke može prikupljati samo sakupljač podataka, kada se poštuju strogi zakonski uslovi.

U skladu sa članom 7 Direktive o zaštiti podataka, lični podaci se mogu prikupljati i obrađivati kada: (i) je pojedinac nedvosmisleno dao svoj pristanak, nakon što je adekvatno informisan/a o posjedovanju podataka; (ii) se obrada posebnih podataka zahtijeva kao dio nekog ugovora; (iii) se obrada podataka zakonski zahtijeva; (iv) je obrada podataka neophodna da bi se zaštitili vitalni interesi pojedinca, na primjer: medicinski podaci žrtve neke nesreće; (v) je obrada podataka neophodna za obavljanje zadataka od javnog interesa; (vi) je prikupljanje podataka neophodno za obavljanje zadataka od javnog interesa, ili zadataka koje sprovodi vlada, poreski organi, policija ili drugi javni organi; (vii) kontrolor podataka ili treća strana ima legitimni interes za prikupljanje ili obradu podataka, pod uslovom da taj interes ne pogađa interese subjekta podataka, ili zadire u njegova/njena osnovna prava, posebno pravo na privatnost. Ova odredba uspostavlja potrebu da se pogodi razumna ravnoteža između poslovnih interesa kontrolora podataka i privatnosti subjekata podataka.

Dok je član 7 dosta sveobuhvatan u pogledu obezbjeđenja uslova za to kada je zakonito da sakupljač podataka sakuplja i obrađuje podatke, treba primijetiti da član 8 Direktive o zaštiti podataka daje dalja pravila. Prema članu 8, postoji zabrana obrade ličnih podataka koji otkrivaju rasno ili etničko porijeklo, politička mišljenja, vjerska ili filozofska vjerovanja, sindikalno članstvo, te onih koji se tiču zdravlja ili seksualnog života, ukoliko ne bude zadovoljen jedan od kriterijuma za izuzimanje iz člana 7.

U pokušaju da se pruži veća zaštita subjektima podataka, i da se odrazi dobra poslovna praksa koja doprinosi pouzdanoj i efikasnoj obradi podataka, Direktiva o zaštiti podataka, takođe, nameće zakonske obaveze sakupljačima podataka, onda kada sakupe lične podatke.

U skladu sa članom 6 Direktive o zaštiti podataka, kontrolori podataka moraju osigurati da: (i) lični podaci budu obrađeni na zakonit i pravičan način; (ii) podaci budu prikupljani za eksplicitne i legitimne svrhe, i korišćeni u skladu sa tim; (iii) količina prikupljenih ili obrađenih podataka bude adekvatna, a ne pretjerana u odnosu na svrhe radi kojih se prikupljaju; (iv) podaci budu precizni; (v) olakšaju ispravku, uklanjanje ili blokiranje netačnih podataka od strane subjekata podataka; (vi) se podaci, koji identifikuju pojedince, ne čuvaju duže nego što je zaista potrebno; (vii) štite lične podatke od slučajnog ili nezakonitog uništavanja, gubitka, izmjene i objelodanjivanja; te konačno da (viii) zaštitne mjere osiguraju nivo zaštite koji odgovara podacima.

Direktiva, dakle, pruža široku zaštitu subjektima podataka: kontrolori podataka su ograničeni uskim okolnostima u kojima mogu da prikupljaju i obrađuju podatke, a takođe i obavezama, koje predviđaju uslovi, nakon prikupljanja ili obrade podataka nekog pojedinca.

iv. Prava subjekata podataka i pravni lijekovi za zloupotrebu podataka

U skladu sa članovima 12 - 21 Direktive o zaštiti podataka, subjekti podataka imaju određeni broj prava u odnosu na kontrolore podataka. Ta prava uključuju pravo na pristup podacima; pravo na prigovor; i obaveze obavještavanja. U veoma širokom smislu, ovaj režim se može objasniti na način na koji je to izloženo u tekstu koji slijedi.

Subjekti podataka: (i) imaju pravo da znaju ime kontrolora koji je sakupljao ili obrađivao njihove podatke; (ii) imaju pravo da znaju svrhu u koju će se upotrijebiti prikupljanje ili obrada podataka; i (iii) imaju pravo da znaju kome se njihovi podaci mogu prenijeti. Subjekti podataka, takođe, imaju pravo da primaju gorepomenute informacije, bilo da su podaci dobijeni neposredno, ili posredno, ukoliko dobijanje takvih infromacija nije nemoguće, neproporcionalno, ili zakonski zabranjeno. Subjekti podataka, nadalje, imaju pravo da naprave kopije svojih podataka, koje je kontrolisao ili obrađivao neki kontrolor podataka, u razumljivoj formi; a imaju i pravo da zahtijevaju brisanje, blokiranje ili potpuno eliminisanje podataka.

Kada su podaci koje je obradio ili prikupio kontrolor podataka netačni, subjekat podataka može: (i) zatražiti od kontrolora da ispravi netačne podatke; i (ii) zahtijevati da kontrolor obavijesti one koji su već vidjeli netačne podatke, opet, ukoliko to ne zahtijeva neproporcionalan napor. Ukoliko subjekat podataka ne dobije adekvatan odgovor od kontrolora, ima pravo da podnese tužbu nacionalnom nadzornom organu za zaštitu podataka. Subjekat podataka, takođe, može uložiti žalbu kontroloru podataka, ukoliko smatra da su njegovi/njeni podaci iskompromitovani; ili ukoliko rukovanje podacima, od strane kontrolora, nije zadovoljavajuće.

v. Prenos podataka

U skladu sa članom 25 Direktive o zaštiti podataka, podaci se mogu prenijeti državama izvan EU, kada se *garantuje adekvatan nivo zaštite*. Član 26 predviđa odstupanja od člana 25, koja uveliko odražavaju kriterijume za odstupanje iz člana 7 Direktive o zaštiti podataka.

b. Okvirna odluka 2008/997/JHA (Okvirna odluka)

Kao što je prethodno pomenuto, pitanja vezana za državnu sigurnost i krivično pravo izlaze izvan okvira Direktive o zaštiti podataka. Okvirna odluka 2008/997/2008 o evropskom nalogu za prikupljanje dokaza, međutim, daje evropska pravila koja se tiču prenosa predmeta, dokumenata i podataka iz druge države članice, za svrhe koje se tiču krivičnog prava.

i. Značenje Evropskog naloga za prikupljanje dokaza, ciljevi Okvirne odluke i opšte definicije

Prema Okvirnoj odluci, Evropski nalog za prikupljanje dokaza je sudska odluka, putem koje se predmeti, dokumenti i podaci mogu dobiti od i biti prenesene drugoj državi članici, u strogo definisanim okolnostima. Cilj Okvirne odluke, dakle, čini se da podstiče saradnju u krivičnim i sudskim istragama.

Član 2 Okvirne odluke daje definicije termina koji se koriste širom Okvirne odluke. Za potrebu

ovog polaznog dokumenta, *država izdavanja* znači državu članicu u kojoj je izdat Evropski nalog za prikupljanje dokaza; a *država izvršenja* znači državu članicu na čijoj teritoriji su locirani predmeti, dokumenti ili podaci ili, u slučaju elektronskih podataka, direktno dostupni prema zakonima države izvršenja.

ii. Opseg Okvirne odluke

Član 4 Okvirne odluke predviđa da Evropski nalog za prikupljanje dokaza može biti izdat kada uslovi iz člana 7 budu zadovoljeni, pod uslovom da traženi predmeti, dokumenti ili podaci budu prikupljeni u skladu sa jednom od svrha navedenih u članu 5.

Međutim, važno je primijetiti da postoji određeni broj okolnosti u kojima Evropski nalog za prikupljanje dokaza ne može biti izdat. Prema članu 4 (2) Evropski nalog za prikupljanje dokaza neće biti izdat u svrhu zahtijevanja od izvršnih vlasti da: (a) sprovedu intervjue, uzmu iskaze; (b) izvrše tjelesne preglede, ili dobiju tjelesni materijal, ili biometrijske podatke; (c) dobiju informacije u realnom vremenu, kao što je prikriveni nadzor ili presretanje komunikacija; (d) sprovedu analizu postojećih predmeta, dokumenata ili podataka; (e) dobiju komunikacijske podatke, zadržane od strane pružalaca usluga javno dostupnih elektronskih komunikacija, ili javnih komunikacijskih usluga.

Takođe je veoma važno primijetiti da Okvirna odluka daje detalje pravila koja se tiču prenosa podataka između država članica. Ona, dakle, ne reguliše aktivnosti obrade podataka od strane policije i pravosudnih organa na nacionalnom nivou. Države članice, stoga, imaju slobodu da određuju svoja vlastita pravila koja se tiču obrade podataka, kao i zaštite podataka u odnosu na krivični postupak, pod uslovom da sprovedena pravila poštuju evropsko pravo države i obaveze iz Evropske konvencije o ljudskim pravima.

iii. Vrste postupaka za koje se može izdati Evropski nalog za prikupljanje dokaza

Kao što je gore objašnjeno, kada to nije posebno isključeno članom 4 Okvirne odluke, slijedi da Evropski nalog za prikupljanje dokaza može biti izdat, jedino, ako je ispoštovan član 7, a izdaje se: (a) u odnosu na krivični postupak, pokrenut pred pravosudnim organom, za krivično djelo prema nacionalnom pravu države izdavanja; (b) u postupku, pokrenutom pred upravnim ili pravosudnim organima, za djela kažnjiva prema nacionalnom pravu države izdavanja, zbog kršenja vladavine prava; (c) gdje odluka može dovesti do postupka pred sudom koji je nadležan u posebnim krivičnim stvarima; i (d) u vezi sa postupkom na koji se odnose tačke (a) – (c), koje se odnose na krivična djela ili kršenja, za koja se pravno lice može smatrati odgovornim ili biti kažnjeno u državi izdavanja.

Evropski nalog za prikupljanje dokaza se, međutim, može izdati u postupcima koji se tiču ličnih podataka, u usko definisanim okolnostima. Član 10 predviđa da se lični podaci, dobijeni po osnovu Okvirne odluke, mogu koristiti od strane države izdavanja, jedino: (a) u svrhu postupka za koji se nalog može izdati; (b) u svrhu drugih sudskih i upravnih postupaka, direktno vezanih za postupke na koje se odnosi tačka (a); (c) u cilju sprječavanja neposredne i ozbiljne prijetnje po javnu sigurnost; i (d) gdje postoji pristanak subjekta podataka.

iv. Uslovi za izdavanje Evropskog naloga za prikupljanje dokaza

Kada se utvrdi da član 4 Okvirne odluke ne isključuje izdavanje naloga, te da je vrsta postupka ona za koju se nalog može izdati, neophodno je uzeti u obzir da li su ispoštovani uslovi za izdavanje naloga, sadržani u članu 7.

U tom smislu, član 7 predviđa da države članice preduzimaju potrebne mjere kako bi osigurale da se Evropski nalog za prikupljanje dokaza izdaje samo onda kada se organ izdavanja zadovoljio da su ispunjeni sljedeći uslovi: (a) dobijanje traženih predmeta, dokumenata ili podataka je neophodno i proporcionalno svrsi postupka na koju se poziva član 5; i (b) predmeti, dokumenti ili podaci se mogu dobiti na osnovu zakona države izdavanja u uporedivom slučaju, ukoliko su bili dostupni na teritoriji države izdavanja, iako bi se mogle koristiti različite proceduralne mjere.

v. Prenošenje Evropskog naloga za prikupljanje dokaza

Prema članu 8 Okvirne odluke, Evropski nalog za prikupljanje dokaza se može prenijeti nadležnom organu države članice kada nadležni organ države izdavanja ima razumnih osnova da vjeruje da su relevantni predmeti, dokumenti ili podaci locirani, ili direktno dostupni, prema zakonima države izvršenja. Ako postoji bilo koji od ovih uslova, informacije će se, bez odlaganja, prenijeti od organa izdavanja do organa izvršenja, bilo kojim sredstvom, koje može da proizvede pisani trag. Treba, međutim, primijetiti da će, prema članu 11, organ izvršenja priznati Evropski nalog za prikupljanje dokaza, prenesen u skladu sa članom 8, ukoliko organ ne odluči da se pozove na bilo koji od osnova nepriznavanja, neizvršenja ili odlaganja, predviđenih u članovima 13 ili 16 Okvirne odluke.

vi. Nepriznavanje, neizvršenje i odlaganje

Prenos predmeta, dokumenata i podataka, međutim, nije jednosmjeran proces u kojem država izvršenja traži i dobija informacije, pod uslovom da su ispoštovani striktni uslovi Okvirne odluke; država izdavanja može odbiti da prizna, izvrši ili odloži prenos Evropskog naloga za prikupljanje dokaza.

U skladu sa članovima 13 i 16 Okvirne odluke, priznanje ili izvršenje ovog naloga može biti odbijeno u državi izvršenja: (a) ukoliko bi njegovo izvršenje kršilo načelo *ne bis in idem*; (b) ukoliko imunitet ili privilegija, po osnovu zakona države izvršenja, onemogućavaju izvršenje naloga; (c) ukoliko se nalog odnosi na krivično djelo za koje se, prema zakonima države izvršenja, smatra da je izvršeno u potpunosti ili većim ili značajnijim dijelom, unutar njene teritorije, ili na mjestu koje je ekvivalent njene teritorije, ili izvan teritorije države izdavanja, ili ukoliko zakon države izvršenja ne dozvoljava pokretanje zakonskog postupka u odnosu na ona krivična djela koja su izvršena izvan teritorije te države; i (d) ako bi izvršenje naloga nanijelo znatnu štetu interesima nacionalne sigurnosti, ugrozilo izvor informacija, ili uključilo korišćenje povjerljivih informacija vezanih za posebne obavještajne aktivnosti.

Nadalje, u skladu sa članom 16, izvršenje Evropskog naloga za prikupljanje dokaza može biti odloženo u državi izvršenja kada: (a) bi njegovo izvršenje moglo ugroziti krivičnu istragu ili gonjenje koje je u toku, do momenta kada država izvršenja to smatra razumnim; ili (b) ako se

predmeti, dokumenti ili podaci, koji su u pitanju, već koriste u drugom postupku, sve dok isti ne budu više potrebni za tu svrhu.

c. Povelja EU o osnovnim pravima

Povelja EU o osnovnim pravima, takođe, predviđa zaštitu ličnih podataka u svom članu 8. Sudska praksa, koja se odnosi na Povelju, je, međutim, veoma ograničena, i stoga se sugeriše da će član 8 biti tumačen tako da održava odredbe Direktive o zaštiti podataka.

d. Budućnost zaštite podataka u Evropskoj uniji

Dana 25. januara 2012. godine, Evropska komisija je predložila sveobuhvatnu reformu Direktive o zaštiti podataka, i uopštenija pravila o zaštiti podataka EU, u odnosu na krivične istrage i obradu podataka.

i. Reforma Direktive o zaštiti podataka

Prema mišljenju Komisije, tehnološki napredak i globalizacija su, umnogome, promijenili način na koji se podaci prikupljaju, procjenjuju i koriste. Komisija, takođe, smatra da su razlike u sprovođenju Direktive o zaštiti podataka u državama članicama rezultirale divergencijama u sprovođenju. Zbog toga, Komisija smatra da je reforma neophodna.[15]

Prijedlozi Komisije pokušavaju da: ažuriraju i osavremene načela, sadržana u Direktivi o zaštiti podataka, kako bi se garantovala prava privatnosti; osnaže unutrašnje tržište EU; osiguraju pravilno sprovođenje pravila za zaštitu podataka; olakšaju međunarodne transfere ličnih podataka; te postave standarde globalne zaštite. Komisija, takođe, predlaže da bude jedan set pravila za zaštitu podataka, i jedan organ odgovoran za zaštitu podataka – nacionalni organ države članice, u kojem se nalazi glavno sjedište kontrolora podataka. Komisija smatra da će ovaj „one stop shop" za zaštitu podataka uveliko pojednostaviti način na koji poslovna zajednica i građani stupaju u interakciju sa zakonima o zaštiti podataka i, stoga, dati podsticaje za trgovinu na međunarodnom tržištu.[16]

ii. Zaštita podataka u krivičnim stvarima

Dana 25. januara 2012. godine, Komisija je, takođe, predložila novu direktivu o zaštiti pojedinaca, s obzirom na obradu ličnih podataka od strane nadležnih organa, u svrhu sprječavanja, istrage, otkrivanja ili gonjenja počinilaca krivičnih djela, ili izvršenja krivičnih sankcija, i slobodnog kretanja tih podataka.

Prema mišljenju Komisije, opseg Okvirne odluke 2008/977/JHA je ograničen, u smislu da se ne primjenjuje na aktivnosti obrade podataka od strane policije i pravosudnih organa na nacionalnom nivou. Prema mišljenju Komisije, ograničeni opseg Okvirne odluke može stvarati poteškoće

15 Vidi Memo/12/41: http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/12/41&format=HTML&aged=0&language=EN&guiLanguage=en

16 *Ibid.*

policiji u vezi sa pravosudnom saradnjom u krivičnim stvarima. Komisija, posebno, smatra da je za organe vlasti teško da naprave jasnu razliku između pitanja domaće i prekogranične obrade.[17]

Komisija je, dakle, predložila ovu direktivu čija intencija je, u skladu sa članom 1 Prijedloga, da pruži pravila vezana za zaštitu pojedinaca u odnosu na obradu ličnih podataka od strane nadležnih organa, u svrhu sprječavanja, istrage, otkrivanja ili gonjenja počinilaca krivičnih djela, ili izvršenja krivičnih sankcija. Član 1, takođe, navodi da Direktiva ima za cilj da osigura da države članice štite osnovna prava i slobode fizičkih lica, istovremeno osiguravajući da razmjena ličnih podataka od strane nadležnih organa, unutar Unije, ne bude ograničena, ni zabranjena.

Član 2 predviđa namjeru Komisije da opseg Direktive bude veći od onog koji ima Okvirna odluka. Komisija predlaže da bi nova direktiva trebalo da se proteže na: (a) obradu ličnih podataka od strane nadležnih organa, za svrhe na koje se odnosi član 1 (1); (b) obradu ličnih podataka u potpunosti ili djelimično korišćenjem automatskih sredstava; i (c) obradu, sredstvima koja nisu automatska, ličnih podataka, koji su sastavni dio, ili su namijenjeni da budu sastavni dio sistema za arhiviranje. Važno je primijetiti da je Komisija predložila da se Direktiva ne primjenjuje na obradu ličnih podataka tokom bilo koje aktivnosti koja, međutim, izlazi iz opsega prava Unije: u tom smislu, najznačajniji izuzetak su pitanja koja se tiču nacionalne sigurnosti.

iii. Sprovođenje

Prijedlozi Komisije će biti predati Evropskom parlamentu i državama članicama EU na raspravu. Predložena Regulativa će biti primjenjiva u svim državama članicama dvije godine nakon što bude usvojena od strane Unije; a države članice će imati period od dvije godine da transponuju odredbe predložene direktive u nacionalno pravo, onda kad Direktiva bude usvojena.

17 http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_10_en.pdf

ZAKLJUČCI i PREPORUKE

U Crnoj Gori se uočava stepen političkog značaja zaštite prava na privatnost i zaštite ličnih podataka. Stepen pravne zaštite prava na privatnost, bez sumnje, mora biti puno veći. Kad se to misli, onda se misli i na unapređenje zakonodavnog okvira, ali još više na stepen zaštite u praksi. Svakako da stepen zaštite ne može biti dovoljno visok, ako ne postoje volja odgovornih, materijalna sredstva i kulturni ambijent. Što se tiče ekonomskog razvoja, on isto tako, dijelom, utiče na unapređenja zaštite privatnosti, jer investitori, koji dolaze iz razvijenog demokratskog svijeta, daju posebnu pažnju ovom pitanju. Političkog napretka, posebno onog koji se tiče evropskih integracija, ne može biti bez napretka u zaštiti prava na privatnost, to je, bez dileme, jedan od evropskih prioriteta.

Razvoj informacione tehnologije dovodi do napretka jedne zemlje u mnogim oblastima. Imperativni zahtjev za poštovanjem prava na privatnost i zaštite istog su potencijalno ugroženi od nekontrolisanog korišćenja informacione tehnologije, bilo od strane države, bilo drugih subjekata. Demokratskog razvoja ne može biti ako se ne postigne kompromis sa slobodom građana.

Takođe, nema ni poštovanja prava na pravično suđenje, ukoliko pojedinac nema dovoljno garancija i mjera zaštite od moguće zloupotrebe od strane državnih organa, kada je u pitanju pravo na privatnost. Kada se ovo kaže onda se, prije svega, misli na sudsku kontrolu pribavljanja predmetnih podataka.

Imajući u vidu sve rečeno, predlažemo sljedeće preporuke koje bi, prema mišljenju CEDEM-a i AIRE Centra, bile od koristi za unapređenje zaštite prava na privatnost u dijelu koji se odnosi na tajnost pisama i drugih sredstava opštenja:

- Inicirati izmjenu Zakonika o krivičnom postupku, na način što će se uvesti odredba koja će obavezivati da za pribavljanje podataka iz telekomunikacionog saobraćaja mora postojati sudska naredba;
- Da se u ZKP-u propiše da svi podaci, koji su dobijeni od operatera, a tiču se telekominikacionog saobraćaja, moraju biti uništeni nakon okončanja postupka predviđenog ZKP-om. Predlažemo da se način uništavanja predvidi po uzoru na postupak kod materijala pribavljenih mjerama tajnog nadzora (MTM);
- Da se u ZKP-u propiše da je, i kod prikupljanja podataka o telekomunikacionom saobraćaju, policija, kao i kod MTN, obavezna da dostavi izvještaj tužiocu, a ovaj sudu o pribavljenom materijalu;
- Da se u ZKP-u propiše da, i kada se radi o prikupljanju podataka iz telekomunikacionog saobraćaja, kao i kod MTN, sudija za istragu, pored naredbe kojom određuje ovu mjeru, izdaje i *poseban nalog* u kojem se navodi samo telefonski broj lica na koje se, prikupljanje podataka o telekomunikacijskom saobraćaju, odnosno mjera tajnog nadzora odnosi, tj. samo e-mail adresa tog lica. Takav nalog policija, potom, predaje pravnom licu koje se bavi pružanjem usluga iz oblasti telekomunikacija;
- Da se u ZKP-u propiše da može postojati mogućnost da se, bez sudskog naloga, prikupe podaci od operatera, uz usmenu naredbu sudije za istragu ili državnog tužioca, ali se pisana naredba mora pribaviti u zakonskom roku;

- Da se ugovori između UP i Operatera baziraju na ustavnoj garnciji nepovredivosti pisama i drugih sredstava opštenja, dok se ne izmijeni ZKP, te da se do tada obavezno pribavlja naredba suda;
- Da se Ustavni sud odredi prema tome da li je u skladu sa Ustavom odredba 257 ZKP, ukoliko se ne bi prihvatili naprijed navedeni predlozi.