CENTRE FOR INTEGRITY IN THE DEFENCE SECTOR

PRISTUP INFORMACIJAMA OD JAVNOG ZNAČAJA I TAJNOST PODATAKA U CRNOJ GORI – ANALIZA PROPISA I NJIHOVE MEĐUSOBNE (NE)USKLAĐENOSTI SA PRAKTIČNIM PREPORUKAMA ZA UNAPREĐENJE U SEKTORU BEZBEDNOSTI

Ana Knežević Bojović

2021. godine

Uvodne napomene

Analiza je usmerena na regulatorni okvir koji se odnosi na informacije od javnog značaja i tajnost podataka u Crnoj Gori, te na praktične probleme i izazove u njihovoj primeni. Predlozi za unapređenje propisa i prakse zasnovani su na međunarodnim standardima i relevantnim i primenjivim dobrim uporednim praksama. Analizu i predloge treba razumeti kao početnu tačku u formulisanju izmena i dopuna postojećeg regulatornog okvira i "mekog prava", u cilju dostizanja jedinstvenosti i koherentnosti unutar sistema, uz uvažavanje njegovih specifičnosti i potreba sistema, naročito u kontekstu nasleđa kulture tajnosti.

- *Zakon o pristupu informacijama od javnog značaja sadrži odredbe koje nisu u skladu sa međunarodnim standardima, dok njegove odredbe nisu međusobno usklađene. Neophodno je temeljno revidirati pravni okvir za pristup informacijama od javnog značaja kako bi se adekvatno regulisala i podstakla transparentnost rada javnog sektora*
- *Zakon o tajnosti podataka ne daje dovoljno jasne smernice u pogledu načina određivanja stepena tajnosti podataka, što znači da su ostavljena relativno široka diskreciona ovlašćenja za klasifikaciju podataka. Bilo bi uputno da se za ceo javni sektor i/ili za sektor odbrane usvoje posebni podzakonski akti ili instrumenti mekog prava, kojima bi se ova oblast detaljnije uredila. Na taj način bi se pružila podrška licima koja odlučuju o klasifikovanju dokumenata, uz istovremeno jačanje integriteta u ovom sektoru*
- *Neophodna su dodatna usaglašavanja pravnih režima za pristup informacijama od javnog značaja i klasifikaciju podataka, uz jasnije regulisanje njihovog međusobnog odnosa*
- *Neophodno je dodatno unaprediti pravila koja se odnose na klasifikaciju podataka u postupcima javnih nabavki, naročito u postupcima javnih nabavki u bezbednosnom sektoru, kako bi se postigla optimalna ravnoteža između potrebe čuvanja poverljivosti tajnih podataka i prava javnosti da zna.*

1. PRISTUP INFORMACIJAMA OD JAVNOG ZNAČAJA

Pravo na pristup informacijama regulisano je Ustavom Crne Gore. Članom 51. Ustava

propisano je da svako ima pravo pristupa informacijama u posedu državnih organa i organizacija koje vrše javna ovlašćenja. Ustavom je propisano da se pristup informacijama može ograničiti ako je to u interesu zaštite života, javnog zdravlja, morala i privatnosti, vođenja krivičnog postupka, bezbednosti i odbrane Crne Gore, spoljne, monetarne i ekonomske politike. Detaljnija ograničenja sadržana su u Zakonu o slobodnom pristupu inofrmacijama.s[1]

Prema RTI rangiranju,[2] Crna Gora zauzima najnižu poziciju od svih država Zapadnog Balkana – 51. mesto sa ukupno 89 od mogućih 150 bodova. Ipak, treba napomenuti da se rangiranje odnosi na prethodni crnogorski zakon, koji je u međuvremenu pretrpeo izmene koje ga u nekim aspektima čine usklađenijim sa relevantnim međunarodnim standardima, dok ga u drugim aspektima od ove usklađenosti udaljavaju.

Naime, 2017. godine Zakon o slobodnom pristupu informacijama[3] izmenjen je tako da njegova primena obuhvati i ponovnu upotrebu informacija, a u skladu sa odgovarajućim pravnim tekovinama Evropske unije.[4] Međutim, drugim izmenama je učinjen značajan korak u nazad u odnosu na režim slobodnog pristupa informacijama, tako je propisano da se odredbe Zakona o slobodnom pristupu informacijama ne primenjuju na određene kategorije podataka, i to:

1) stranke u sudskim, upravnim i drugim na zakonu propisanim postupcima, kojima je pristup informacijama iz tih postupaka utvrđen propisom

2) informacije za koje postoji obaveza čuvanja tajne, u skladu sa zakonom koji uređuje oblast tajnih podataka

3) informacije koje predstavljaju klasifikovane informacije čiji su vlasnici međunarodne organizacije ili druge države, te klasifikovane informacije organa vlasti koje nastaju ili se razmenjuju u okviru saradnje s međunarodnim organizacijama ili drugim državama.

Činjenica da su Zakonom o slobodnom pristupu informacijama od javnog značaja od njegove primene *a priori* izuzeti svi oni podaci koji su označeni kao tajni u skladu sa odgovarajućim zakonom, bez mogućnosti da se u svakom konkretnom slučaju primeni test štetnosti i mogućnosti da se naloži deklasifikacija informacija, predstavljaju značajno odstupanje od relevantnih

[1] Sl. list Crne Gore", br. 44/12 i 30/2017, član 14.
[2] http://www.rti-rating.org/. RTI rangiranjem ocenjuje se kvalitet regulatornog okvira pojedinačnih država u oblasti pristupa informacijama.
[3] Zakon o izmjenama i dopunama Zakona o slobodnom pristupu informacijama, Sl. list Crne gore 30/2017.
[4] Directive 2013/37/EU of the European Parliament and of the Council of 26 June 2013 amending Directive 2003/98/EC on the re-use of public sector information.

međunarodnih standarda. Nadalje, formulacija prema kojoj se odredbe Zakona o slobodnom pristupu informacijama ne primenjuju na stranke u sudskim, upravnim i drugim na zakonu propisanim postupcima izuzetno je široka. Iako je prema međunarodnim standardima ograničavanje pristupa informacijama kako bi se sačuvala poverljivost sudskih i drugih postupaka, te obezbedila ravnopravnost stranaka u postupku jeste prepoznato kao dozvoljeno ograničenje, ono nije apsolutno i praćeno je sprovođenjem testa štetnosti i testa javnog interesa. Suprotno ovom međunarodnom standardu, Crna Gora je ovo ograničenje postavila na izrazito neodređen način, što može voditi velikom broju zloupotreba. Takođe, postavlja se pitanje opravdanosti uvođenja ovog izuzetka od primene, budući da je ostalim odredbama Zakona o slobodnom pristupu informacijama jasno propisano da se pristup podacima koji se odnose na prevenciju, istrage i gonjenje učinilaca krivičnih dela, te pokretanje i vođenje dispilinskog postupka može ograničiti. Budući da Zakonom o izmenama o dopunama ove odredbe nisu brisane, stvorena je dodatna konfuzija u pogledu toga na koje će se upravne, sudske i druge zakonom propisane postupke (postupci medijacije, ali i postupci izbora sudija ili postupci po javnom oglasu?) ovo izuzeće primenjivati i kako će se ono razlikovati od krivičnog postupka, istrage i disciplinskog postupka. I ovo ograničenje je nesumnjivo prekomerno u odnosu kako na međunarodne standarde, tako i u odnosu na ograničenja propisana Ustavom, te ih iz Zakona o slobodnom pristupu informacijama treba brisati. Isto važi i za podatke koji su označeni kao tajni, koji su sada članom 1. Zakona izuzeti iz primene, ali istovremeno su zadržane odredbe prema kojima je moguće ograničiti pristup informacijama u interesu zaštite bezbenosti, spoljne, monetarne i ekonomske politike, u skladu sa propisima kojima se uređuje tajnost podatka.

Otuda se mora zaključiti da regulatorni okvir Crne Gore nije u skladu sa međunarodnim standardima u pogledu svog obuhvata i da su u njemu potrebna značajna unapređenja. Ovom priliku koristimo priliku i da se osvrnemo na činjenicu da su ne samo loša rešenja crnogorskog zakona, već i negativna praksa tajnosti, bile predmet temeljnih i ozbiljnih analiza i kritika stručne javnosti.[5]

I inače su ograničenja slobode pristupa informacijama od javnog značaja u Crno j Gori propisana na nekonzistentan način. Naime, za razliku od većine pravnih sistema u regionu, Crna Gora se

[5] Videti naročito analize dostupne na https://www.mans.co.me/tag/zakon-o-slobodnom-pristupu-informacijama/

opredelila da ova ograničenja propiše već u Ustavu. Osim što se načelno može postaviti pitanje da li je pitanje dozvoljenih ograničenja slobodnog pristupa informacijama materio constitutionis ili ne, pristup crnogorskog ustavopisca nalaže da i ograničenja propisana zakonom budu usklađena sa ustavnim rešenjem. Ipak, i u pogledu obuhvata ustavom propisanih ograničenja, kao i u pogledu međusobne usklađenosti ustavnih i zakonskih normi, može se ukazati na određene manjkavosti. U tabeli ispod dat je uporedni pregled normi ustava i zakona.

Ustav	Zakon o slobodnom pristupu informacijama
Zaštita života	
Javno zdravlje	
Moral i privatnost	Zaštita privatnosti od objelodanjivanja podataka predviđenih zakonom kojim se uređuje zaštita podataka o ličnosti, osim podataka koji se odnose na: - javne funkcionere u vezi sa vršenjem javne funkcije, kao i prihode, imovinu i sukob interesa tih lica i njihovih srodnika koji su obuhvaćeni zakonom kojim se uređuje sprječavanje sukoba interesa, - sredstva dodijeljena iz javnih prihoda, osim za socijalna primanja, zdravstvenu zaštitu i zaštitu od nezaposlenosti;
Vođenje krivičnog postupka	Prevencija istrage i gonjenje izvršilaca krivičnih djela, radi zaštite od objelodanjivanja podataka koji se odnose na: - sprječavanje izvršenja krivičnog djela, - prijavljivanje krivičnog djela i njegovog izvršioca, - sadržinu preduzetih radnji u pretkrivičnom i krivičnom postupku, - dokaze prikupljene izviđajem i istragom, - mjere tajnog nadzora, - zaštićenog svjedoka i svjedoka saradnika, - efikasnost vođenja postupka;
Bezbednost i odbrana Crne Gore Spoljna, monetarna i ekonomska politika	Bezbjednosti, odbrana, spoljnja, monetarna i ekonomska politike Crne Gore, u skladu sa propisima kojima se uređuje tajnost podataka, označeni stepenom tajnosti;
	Vršenje službene dužnosti, radi zaštite od objelodanjivanja podataka koji se odnose na: - planiranja inspekcijske kontrole i nadzora od strane organa vlasti, - konsultacije unutar i između organa vlasti u vezi sa utvrđivanjem stavova, radi izrade službenih dokumenata i predlaganja rješenja nekog predmeta, - rad i odlučivanje kolegijalnih organa, - pokretanje i vođenja disciplinskog postupka;

	Zaštita trgovinskih i drugih ekonomskih interesa od objavljivanja podataka koji se odnose na zaštitu konkurencije kao i na poslovnu tajnu u vezi sa pravom intelektualne svojine;
	Ako je informacija poslovna ili poreska tajna u skladu sa zakonom

Kao što se može videti, dva režima međusobno nisu u potpunosti usklađena. Zakonom, na primer, ograničenja radi zaštite života i javnog zdravlja uopšte nisu nabrojana niti precizirana. Vrlo široko ustavom postavljeno ograničenje slobode pristupa radi zaštite morala takođe nije detaljnije obrađeno i precizirano u zakonu. Sa druge strane, ograničenja koja se odnose na vođenje krivičnog postupka postavljena su prilično široko i sveobuhvatno. Zakonom su uneta i dodatna ograničenja slobode pristupa informacijama, kao što su poreska i poslovna tajna. Čini se da je očiglednom omaškom ograničenje slobodnog pristupa informacijama po osnovu činjenice da se radi o podacima koji su označene stepenom tajnosti u skladu sa odgovarajućim zakonom zadržana u zakonu, iako su prethodnim odredbama zakona ovi podaci u potpunosi isključeni iz domena primene Zakona o slobodnom pristupu informacijama.

Nadalje, intervencijama zakonodavca za slobodan pristup informacijama od javnog značaja je dodato još jedno ograničenje -ako je informacija poslovna ili poreska tajna u skladu sa zakonom. Ovo rešenje predstavlja značajno ograničenje slobode pristupa informacijama od javnog značaja, budući da ne postoji nijedan propis koji bi na jedinstven način regulisao pojam poslovne tajne, već se pojam poslovne tajne pojavljuje u većem broju propisa, kao što su Zakon o privrednim društvima, Zakon o radu, i slično, a kriterijumi za označavanje nekog podatka kao poslovne tajne su relativno arbitrerni i prepušteni su pojedinačnim organima ili privrednim društvima. U praksi bi to značilo da svemu što neki privredni subjekt označi kao poslovnu tajnu, u skladu sa svojim internim aktom, može uskratiti pristup čak i u slučajevima kada se radi o privrednom subjektu čiji je osnivač neki organ javne vlasti ili je organ javne vlasti njegov isključivi ili većinski vlasnik. Situaciju dodatno komplikuje činjenica da je odavanje poslovne tajne propisano i kao krivično delo Zakonikom o krivičnom postupku[6] jer ovakva odredba, u nedostatku jasnijeg zakonskog određenja, nesumnjivo može imati odvraćajuće dejstvo i uticati na to da se prilikom sprovođenja testa štetnosti i mogućnost krivične odgovornosti uzme u obzir, formalno ili neformalno.

[6] Član 280

Nesumnjivo je korisno je što je poslovna tajna ipak jasno stavljena pod režim Zakona o slobodnom pristupu informacijama, te će se i na nju primenjivati pravila o sprovođenju testa štetnosti te uvrđivanja interesa javnosti da zna. Međutim, praksa iz regiona ukazuje da u pogledu ovog izuzetka mora postojati dodatni oprez, jer se neretko dešavalo da je javnosti uskraćivan pristup informacijama zbog toga što su mnogi podaci označeni kao poslovna tajna privatnog partnera u pravnom poslu koji je od velikog interesa za javnost jer podrazumeva ne samo obim i vrstu ulaganja privatnog partnera, već i izdvajanja države kroz direktne podsticaje i učešće u troškovima (na primer, izgradnje infrastrukture). Zbog svega navedenog, uputnije bi bilo da se zaštita poslovne tajne jasnije i preciznije uredi posebnim propisom. U tom pogledu upućujemo na praksu koja postoji u regionu, odnosno na Zakon o zaštiti poslovne tajne koji je usvojila Srbija[7] i Zakon o Zakon o zaštiti neobjavljenih informacija s tržišnom vrijednosti[8]. Napominjemo da je hrvatskim propisom u nacionalno zakonodavstvo uneta Direktiva (EU) 2016/943 Evropskog parlamenta i Saveta o zaštiti neotkrivenih znanja i iskustva te poslovnih informacija (poslovne tajne) od nezakonitog pribavljanja, korišćenja i otkrivanja[9] te da bi prilikom usvajanja odgovarajućeg crnogorskog propisa trebalo voditi računa o ovoj pravnoj tekovini Evropske unije. Iako je tačno da je Crna Gora još 2007. godine usvojila Zakon o zaštiti neobjavljenih podataka, koji je potom izmenjen 2008. godine, napominjemo da je ovaj zakon stavljen pre svega u kontekst zaštite prava intelektualne svojine. Nasuprot tome, novi evropski *aquis* pitanje poslovne tajne postavlja šire, istovremeno ukazujući da ova direktiva ima primat nad propisima koji se odnose na zaštitu intelektualne svojine, kao *lex specialis* u onim slučejevima kada se polje njihove primene preklapa, kao što je istaknuto u stavu 39 uvodnih izjava Direktive 2016/943.

Novinu u zakonu od 2017. godine predstavlja i ograničenje slobodnog pristupa informacijama po osnovu poreske tajne. Radi se o ograničenju koje nije nepoznato u uporednoj praksi, s tim što se obim ograničenja razlikuje od države do države.[10] U Crnoj Gori, poreska tajna je detaljnije propisana Zakonom o poreskoj administraciji. Članom 16. ovog zakona propisano je da je poreska tajna **svaka informacija ili podatak o poreskom obvezniku** kojim raspolaže poreski organ, osim

[7] Službeni glasnik RS, br. 72/2011
[8] NN 30/18
[9] Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure
[10] Službeni list Republike Crne Gore,br. 20/2011, 28/2012, 8/2015, 47/2017 i 52/2019, član 6, stav 1, tačka 17

informacija i podataka:

1) za koje poreski obveznik pismeno izjavi da se ne smatraju poreskom tajnom;

2) koji se ne mogu povezati sa konkretnim poreskim obveznikom niti se na drugi način mogu identifikovati;

3) koji su vezani za postojanje poreskog duga, ukoliko je sredstvo obezbeđenja upisano u javne knjige;

4) informacije o registraciji poreskog obveznika;

5) informacije o vrednosti nepokretne imovine;

6) informacije koje poreski organ objavljuje kvartalno o listi poreskih dužnika.

Nadalje, ovim zakonom je propisano da se podaci koji predstavljaju poresku tajnu mogu učiniti dostupnim drugom poreskom organu na njegov zahtev.

Čini se da intencija zakonodavca prilikom izrade Zakona o poreskoj administraciji nesumnjivo nije mogla biti da se podacima koji mogu predstavljati poresku tajnu da onakva zaštita kakva se daje podacima čije bi otkrivanje moglo naneti štetne posledicce za bezbednost, odbranu, spoljnu, monetarnu i ekonomsku politiku Crne Gore, te je dobro što je poreska tajna jasno podvedena pod režim Zakona o slobodnom pristupu informacijama. To znači da se prilikom traženja pristupa poreskoj tajni mora sprovoditi test štetnosti kao i test javnog interesa. Ipak, dosadašnja praksa Poreske administracije, kao i Upravnog suda, upućuju na to da su odredbe o poreskoj tajni tumačene tako da činjenica da neka informacija predstavlja poresku tajnju znači da je prilikom sprovođenja testa štetnosti dovoljno navesti tu činjenicu, te da to predstavlja dovoljan test štetnosti. Ovakvo tumačenje nikako ne bi smelo uzeti maha – a nažalost, ono je potvrđeno u sudskoj praksi Upravnog suda. Naime, u svojoj presudi U. 7765/18 od 3. 7. 2019 Upravni sud Crne Gore stao je na sledeće stanovište:

> *Naime, imajući u vidu citirane zakonske odredbe, a polazeći od činjenice da je prvostepeni organ sproveo test štetnosti objavljivanja sporne informacije i utvrdio da bi objelodanjivanje te informacije predstavljalo kršenje Zakona o poreskoj administraciji, kojim se uređuju prava i obaveze poreskog organa i poreskih obveznika u postupku utvrđivanja, naplate i kontrole poreza i drugih dažbina, kao i da se u konkretnom slučaju*

radi o poreskoj tajni, to je i po ocjeni Suda, pravilan zaključak prvostepenog i drugostepenog organa da nije bilo uslova da se dozvoli pristup zahtjevom traženoj informaciji u skladu sa članom 13 Zakona o slobodnom pristupu informacijama.

Navedeno stanovište Upravnog suda nipošto se ne bi moglo oceniti usklađenim sa odgovarajućim međunarodnim standardima.

Na prvi pogled bi se moglo učiniti da je izmenama i dopunama Zakona o slobodnom pristupu informacijama iz 2017. godine uspostavlja dugo željeni red u oblasti pristupa informacijama a državnim službenicima olakšava postupanje. Ipak, potpuno izuzimanje podataka koji su označeni kao tajni iz režima slobodnog pristupa informacijama se nikako ne može smatrati ograničenjem ljudskog prava koje je neophodno u demokratskom društvu – štaviše, ovo znači i potpuni izostanak sudske kontrole nad označavanjem nekog podatka kao tajnog.

Ono što je dobro rešenje jeste neposredno upućivanje na Zakon o zaštiti podataka o ličnosti te Zakon o tajnosti podataka kao izvore prava kojima su regulisana pitanja zaštite privatnosti, odnosno, podataka o ličnosti, i zakona o tajnosti podataka. Ono što međutim, nedostaje, jeste jasno i izričito ukazivanje na to koji će se zakon primenjivati tj. koji zakon će imati primat u slučaju njihove međusobne neusklađenosti. Jedno od mogućih rešenja ovog pitanja bilo **bi postojanje zakonske pretpostavke u pogledu prava javnosti da zna, koje je poznato u uporednom pravu i pravu nekih država u regionu**.[11] Ona se i pretpostavlja u odnosu na pojedine kategorije podataka o ličnosti već u samom zakonu, tako što je izričito propisano koje kategorije podataka ne podležu ograničenju pristupa informacijama po osnovu zaštite privatnosti – kao što su podaci koji se odnose na javne funkcionere u vezi sa vršenjem javne funkcije, kao i prihode, imovinu i sukob interesa tih lica i njihovih srodnika kao i podatke koji se odnose na sredstva dodeljena iz javnih prihoda. Nadalje, Zakonom o slobodnom pristupu informacijama jasno je propisana i ne samo mogućnost već i dužnost organa vlasti da, ako je ograničen pristup delu informacije, taj deo informacije izbriše a omogući uvid preostalom delu informacije.

[11] Kao što je Srbija, čiji Zakon o slobodnom pristupu informacijama od javnog značaja već godinama zauzima jedno od prvih mesta prema RTI rangiranju.

U odnosu na Zakon o tajnosti podataka, sa jedne strane, jezičko tumačenje teksta Zakona o slobodnom pristupu informacijama ukazivalo bi na to da će se u slučaju nesaglasnosti ova dva zakona primenjivati Zakon o tajnosti podataka. Takav zaključak proizilazi i iz činjenice da je Zakonom o slobodnom pristupu informacijama propisano da se prilikom odlučivanja o tome da li će se tražiocu omogućiti pristup informaciji test štetnosti ne sprovodi za podatke koji su označeni stepenom tajnosti.[12] Ovo bi značilo da u tom slučaju postoji zakonska pretpostavka da bi otkrivanje te informacije moglo naneti štetu zaštićenim interesima.

Ipak, nesprovođenje testa štetnosti ne znači i da istovremeno ne može postojati **preovlađujući interes javnosti da zna**, a koji postoji kada tražena informacija sadrži podatake koji osnovano ukazuju na:

1) korupciju, nepoštovanje propisa, nezakonito korišćenje javnih sredstava ili zloupotrebu ovlašćenja u vršenju javne funkcije
2) sumnju da je izvršeno krivično delo ili postojanje razloga za pobijanje sudske odluke;
3) nezakonito dobijanje ili trošenje sredstava iz javnih prihoda;
4) ugrožavanje javne bezbednosti;
5) ugrožavanje života;
6) ugrožavanje javnog zdravlja;
7) ugrožavanje životne sredine.[13]

Ovako određen preovlađujući interes u određenoj meri je podudaran sa razlozima navedenim u članu 4. Zakona o tajnosti podataka zbog kojih se podatak ne može označiti tajnim, to jest radi prikrivanja:

1) izvršenog krivičnog dela
2) ugrožavanje životne sredine
3) ograničavanje konkurencije
4) prekoračenja ili zloupotrebeovlašćenja
5) nezakonitog akta i postupanja
6) administrativne greške organa.

[12] Čan 16, stav 2. Zakona o slobodnom pristupu informacijama
[13] Član 17. Zakona o slobodnom pristupu informacijama

Ipak, razlozi zbog kojih je Zakonom o tajnosti podataka propisano da se neki podatak mora oglasiti tajnim odnose se samo na *post festum* situacije, to jest na situacije u kojima bi označavanje nekog podatka tajnim predstavljalo *prikrivanje*. Nasuprot tome, Zakonom o slobodnom pristupu informacijama uspostavljen javni interes odnosi se u manjoj meri na već okončane situacije ili akte (sumnju da je izvršeno krivično delo) a u većoj meri i na tekuće situacije – ugrožavanje života , ugrožavanje javnog zdravlja, nezakonito trošenje javnih sredstava i uspostavljen je upravo kako bi se neke od ovih štetnih radnji mogle blagovremeno zaustaviti a nastanak štete u potpunosti sprečiti ili smanjiti. Otuda se mora smatrati da postojanje preovlađujućeg javnog interesa predstavlja apsolutni osnov za omogućavanje pristupa informaciji, čak i kada je ona označena stepenom tajnosti.

Nedavna praksa Upravnog suda ukazuje da je i sam Upravni sud nailazio na izazove prilikom ocenjivanja toga koji od dva zakona ima primat, kao i koji član zakona treba primeniti. Ista praksa pokazuje da je sud stao na stanovište da ipak treba primeniti član 14. Zakona, bar u pojedinim slučajevima. Ilustrativna je u tom pogledu Presuda Upravnog suda Crne Gore, U. 2757/18 od 21. 1. 2020. Naime, u ovoj presudi tražen je pristup podacima koji su nesporno označeni oznakom tajnosti u skladu sa Zakonom o tajnosti podataka. Međutim, u obrazloženju svoje presude sud se nije pozvao na apsolutno izuzeće tajnih podataka iz primene Zakona o slobodnom pristupu informacijama od javnog značaja, već je ispitivao da li je za otkrivanje klasifikovanih podataka postojao preovlađujući javni interes.

Podsetimo takođe da je Zakonom o slobodnom pristupu informacijama takođe je propisano da ako se traži pristup inofrmaciji koja sadrži neki podatak označen stepenom tajnosti, potrebno je da se prethodno dobije saglasnost organa koji je odredio tajnost podatka za otkrivanje podatka. U ovom slučaju može doći do nekoliko situacija:
- organ koji je podatak označio tajnim je u međuvremenu ukinuo oznaku tajnosti. U tom slučaju nema potrebe ni za kakvom saglasnošću organa koji je podatak označio tajnim, iako se o ukidanju tajnosti podatka pre isteka vremena obavezno obveštavaju svi organi i organizacije koje koriste taj podatak. U tom slučaju ipak ima potrebe za obaveštavanjem organa kome je podnet zahtev za pristup informaciji da podatak više nije tajan kako bi nadalje organ sprovodio test štetnosti i javnog

interesa kao i za druge podatke u posedu organa javnih vlasti

- organ koji je podatak označio tajnim daje saglasnost za pristup informaciji. Ono što ostaje nejasno i nedorečeno u regulatornom okviru jeste da li je u tom slučaju potrebno ukinuti oznaku tajnosti i da li je organ koji je podatak označio tajnim dužan da to odmah učini – ciljano tumačenje jasno ukazuje da bi ukidanje tajnosti logički prethodilo saglasnosti. Ovakvo tumačenje je utemeljeno i u Zakonu o tajnosti podatka, koji propisuje[14] da ovlašćeno lice može ukinuti tajnost podatka pre isteka vremena na koje je tajnost podatka određena. Ipak, treba uzeti u obzir činjenicu da ako je strešina organa preneo na neko drugo lice ovlašćenje da podatak označi tajnim, prema Zakonu o tajnosti podataka, to lice mora prethodno tražiti saglasnost starešine organa da podatak deklasifikuje.[15]
- organ koji je podatak označio tajnim nije saglasan sa pristupom informaciji. Ovo je možda i ishod koji se najčešće može očekivati. **Ranija praksa Upravnog i Vrhovnog suda[16] jasno su ukazivale na činjenicu da to što na neki podatak stavljena oznaka tajnosti samo po sebi nije dovoljno da se odbije pristup informaciji. Nadalje, čak ni činjenica da organ koji je odredio tajnost podatka nije saglasan sa njegovim objavljivanjem takođe nije dovoljna za odbijanje zahteva za pristup informaciji – organ od koga je pristup informaciji tražen dužan je sprovede test štetnosti pa tek na osnovu njega može odbiti pristup informaciji**. Ovo državne službenike i nameštenike stavlja u težak položaj, budući da sami treba, prema sudskoj praksi, da sprovedu test štetnosti, a takođe i ispitaju postojanje preovlađujućeg interesa javnosti da zna, dok se istovremeno pretpostavlja da je organ koji je podatak označio tajnim ponovno izvršio test štetnosti.[17]

[14] Član 18, stav 2.
[15] Član 18, stav 3.
[16] Presuda Upravnog suda od 8.2. 2016. godine kao i presuda Vrhovnog suda Crne Gore od 22. 1. 2016. godine
[17] "Transparentnost i odbrana u Crnoj Gori", CEMI, str. 19.

- *Na osnovu prethodne analize čini se jasnim da je temeljna reforma Zakona o slobodnom pristupu informacijama neophodna. Pre svega, potrebno je kategorije podataka koje su a priori , i to nedoslednom zakonskom intervencijom, izuzete iz primene Zakona o slobodnom pristupu informacija, temeljno reformisati. Ujedno, preporučujemo da se u Zakon o slobodnom pristupu informacijama uvede i zakonska pretpostavka postojanja javnog interesa za otkrivanjem informacije. Iako se može činiti da ovakva zakonska norma ne bi bila neophodna ukoliko bi se pravni okvir za slobodan pristup informacijama temeljno reformisao, smatramo da bi ovakva norma predstavljala značajan iskorak od postojeće pravne I administrativne kulture u kojoj se favorizuje uskraćivanje pristupa podacima. Istovremeno, smatramo da bi ona predstavljala jasan podsticaj javnom sektoru da u punoj meri prihvati osnovna načela slobodnog pristupa informacijama od javnog značaja.*

Istovremeno, ukazujemo i na sledintervencije koje bi upravo u kontekstu omogućavanja slobodnog pristupa informacijama mogle biti sprovedene u Zakonu o tajnosti podataka:

- *da se oznaka tajnosti vanredno preispituje na osnovu podnetog zahteva za pristup podatku koji je označen tajnim, a na osnovu Zakona o slobodnom pristupu informacijama od javnog značaja u slučaju da organ koji je podatak označio tajnim obavesti organ kome je zahtev podnet da nije saglasan sa zahtevom za pristup podatku, te da se ovo preispitvanje obavlja Komisija*
- *obavezu Komisije koja preispituje oznaku tajnosti da ispita postojanje preovlađujućeg javnog interesa smislu Zakona o slobodnom pristupu informacijama od javnog značaja i*
- *postupanje Komisije u kratkim rokovima.*

Važno je istaći da je Zakonom izričito propisano da sud ima pravo da ceni da li je organ vlasti podatke sadržane u informaciji kojoj se traži pristup pravilno označio stepenom tajnosti.[18] Ukoliko bi se odredbe Zakona o tajnosti podataka izmenile na način predložen u ovom tekstu, onda bi valjalo da se ova odredba dopuni tako glasi "pravilno označio stepenom tajnosti ili nakon vanrednog preispitivanja odlučio da zadrži oznaku tajnosti".

[18] Član 44. Zakona o slobodnom pristupu informacijama.

2. TAJNOST PODATAKA

Zakonom o tajnosti podataka[19] ("Sl. List Crne Gore" br 14/13) propisuje se jedinstven sistem određivanja tajnosti podataka, pristupa tajnim podacima, čuvanja, korišćenja, evidencije i zaštite tajnih podataka. Ova materija je detaljnije i preciznije uređena sledećim podzakonskim aktima:

- Uredba o načinu i postupku označavanja tajnosti podataka[20]
- Uredba o posebnim mjerama zaštite tajnih podataka od značaja za odbranu zemlje[21]
- Uredba o načinu vršenja i sadržaju unutrašnje kontrole nad sprovođenjem mjera zaštite tajnih podataka [22]
- Uredba o evidenciji tajnih podataka[23]
- Uredba o bližim uslovima i načinu sprovođenja informatičkih mjera zaštite tajnih podataka[24]
- Uredba o bližim uslovima i načinu sprovođenja industrijskih mjera zaštite tajnih podataka[25]
- Uredba o bližim uslovima i načinu sprovođenja administrativnih i fizičkih mjera zaštite tajnih podataka[26]
- Pravilnik o sadržini i obliku dozvole za pristup tajnim podacima[27]

Najveći broj podzakonskih akata donet je pre 2012. godine – izuzetak u tom pogledu predstavlja Uredba o bližim uslovima i načinu sprovođenja administrativnih i fizičkih mera zaštite tajnih podataka, koja je usvojena tokom 2015. godine. Napominjemo da je Zakon o tajnosti podataka

[19] Službeni list Crne Gore br. 14/08, 41/10, 40/11, 38/12, 44/12, 14/13, 18/14, 48/15 i 74/2020.
[20] Službeni list Crne Gore 67/2008
[21] Službeni list Crne Gore, br. 48/09
[22] Službeni list Crne Gore br. 48/09
[23] Službeni list Crne Gore br. 67/08 i 49/10
[24] Službeni list Crne Gore, br. 57/10
[25] Službeni list Crne Gore, br. 8/11
[26] Službeni list Crne Gore br. 54/15
[27] Službeni list Crne Gore br. 71/08

izmenjen 2012, 2013, 2014, 2015. i 2020. godine. **To nužno znači da celokupan regulatorni okvir zaštite tajnosti podataka nije postavljen na sistemski zaokružen način i da je neophodno unaprediti ga, te dodatno uskladiti sa Zakonom o slobodnom pristupu informacijama od javnog značaja, kao i dati jasnije smernice u pogledu primene Zakona o tajnosti podataka**. U tom pogledu od ključnog značaja bilo bi **konačno usvajanje podzakonskog akta ili akata kojima bi se detaljnije uredile kategorije podataka koje se označavaju oznakom tajnosti, a u skladu sa postojećim međunarodnim standardima.**

Ponovimo, Zakonom je propisano da se tajnim podacima smatraju podaci su podaci čijim bi otkrivanjem nepozvanom licu nastupile ili mogle nastupiti štetne posljedice za bezbednost i odbranu, spoljnu, monetarnu i ekonomsku politiku Crne Gore. To znači da se tajnost podataka određuje u odnosu na:

- sadržaj podatka

- značaj podatka za zaštićene interese a to su:

    - bezbednost i odbrana

    - spoljna politika

    - monetarna politika

    - ekonomska politika.

Zaštita ekonomske politike ne čini se dovoljno specifičnim razlogom za određivanje tajnosti podatka i otuda može predstavljati osnov za prekomernu upotrebu.

Prema Zakonu, podatak se može označiti tajnim ako je:
- to neophodno u demokratskom društvu i
- ako je interes koji se štiti značajniji od interesa za slobodnim pristupom informacijama.

Iz ovih formulacija mogu se izvesti sledeći zaključci:

1. Iako u samom tekstu Zakona o tajnosti podataka kao i u tekstu Zakona o slobodnom pristupu informacijama od javnog značaja nije izričito propisano koji od ova dva zakona će imati primat u primeni u slučaju međusobne neusklađenosti, **ciljno tumačenje gore navedene norme Zakona o**

tajnosti podataka ukazuje da Zakon o slobodnom pristupu informacijama od javnog značaja ima primat nad Zakonom o tajnosti podataka. Ovo otud što je zakonodavac već u samom tekstu norme ukazao da je za označavanje podatka tajnim neophodno da je interes koji se štiti značajniji od interesa za slobodnim pristupom informacijama. Budući da se radi samo o ciljnom tumačenju, kako bi se obezbedila njegova puna primena bilo bi uputno u budućim **zakonskim odrebama, podzakonskim aktima ili instrumentima tzv. mekog prava (smernice, vodiči) ukazati na primat Zakona o slobodnom pristupu informacijama od javnog značaja nad Zakonom o tajnosti podatak**a.

2. Da obrazloženo rešenje kojim se podatak označava tajnim i određuje stepen njegove tajnosti treba da sadrži:

- test štetnosti i test javnog interesa
-test proporcionalnosti.

Ovo je izuzetno značajno za praksu određivanja tajnosti podataka, a istovremeno i za potpunije razumevanje odnosa između Zakona o tajnosti podataka i Zakona o slobodnom pristupu informacijama od javnog značaja.

Naime, kako je već objašnjeno, ograničenja pristupa informacijama od javnog značaja moguća su u slučajevima određenim zakonom, i to ukoliko se utvrdi da bi njihovim otkrivanjem nastupila šteta za zaštićene interese koja je veća od interesa javnosti da zna. Iz odredbi Zakona o tajnosti podataka proizilazi da su razlozi za određivanje tajnosti podataka istovetni kao i oni za uskraćivanje pristupa podacima od javnog značaja, te da je u odnosu na Zakon o slobodnom pristupu informacijama ključna razlika u zaštićenim interesima.

Nadalje, iz ovih odredbi jasno proizilazi da obrazloženje ovog rešenja ne može sadržati samo pozivanje na odgovarajuće odredbe Zakona, već da mora **sadržati i test štetnosti i javnog interesa i to u svakom konkretnom slučaju**. Moramo napomenuti da je praksa Upravnog suda, kao što je napomenuto u analizi koja se odnosi na Zakon o slobodnom pristupu informacijama, poslednjih godina išla za prilično formalističkim, čak i površnim tumačenjem sadržine testa štetnosti, stajući na stanovište da je za štetnost objavljivanja dovoljno pokazati da se radi o informaciji koja je nekim propisom – ne nužno Zakonom o tajnosti podataka – određena kao jedna od brojnih kategorija tajne. Neophodno je da crnogorski državni organi i organizacije, kao i sudovi, ubuduće odstupe od ovakvog tumačenja.

Prema Zakonu, izuzetak od pravila da se test štetnosti i test javnog interesa moraju sprovesti u svakom konkretnom slučaju predstavlja situacija kada se u nekom organu u kontinuitetu nastaju i ponavljaju se istovrsni tajni podaci – da lice ovlašćeno za određivanje stepena tajnosti podataka može posebnim aktom označiti te podatke tajnim i odrediti stepen njihove tajnosti.
Ovaj izuzetak, sa jedne strane, predstavlja meru koja ide u prilog efikasnosti postupka određivanja tajnosti podataka. Sa druge strane, i ovaj izuzetak je neophodno tumačiti izuzetno usko, što je i inače osnovno pravno pravilo, iz sledećih razloga:
- ukoliko se radi o podacima koji se kontinuirano pojavljuju, označavanje grupe podataka tajnim značajno utiče na vreme važenja oznake tajnosti i njeno preispitivanje
- automatsko označavanje nekog podatka kao tajnog može dovesti do rutinskog označavanje podatka kao tajnog iako je u međuvremenu došlo do promene usled koje ta kategorija podataka više ne treba da bude tajna
- rutinsko označavanje određenih kategorija podsatak akao tajnih lako može za posledicu imati zloupotrebu.

Činjenica da ovakav izuzetak nije predviđen u propisima o tajnosti podataka država u regionu (Severna Makedonija, Hrvatska, Srbija i Slovenija ne poznaju ovakav izuzetak) ide u prilog poslednjem razlogu zbog koga je istaknuto da se ovaj izuzetak mora tumačiti usko.
U svetlu ranije iznetih konstatacija koje se odnose na režim slobodnog pristupa informacijama u Crnoj Gori – ovde mislimo kako na trenutno važeće propise, tako i na praksu – **preporučujemo da se ovaj izuzetak briše iz Zakona o tajnosti podataka.**

Zakonom je propisano da se tajnom podatku mogu odrediti sledeći stepeni tajnosti:

- "STROGO TAJNO";- za podatke čije otkrivanje bi ugrozilo ili nanelo neotklonjive štetne posledice za bezbjednost i interese Crne Gore
- "TAJNO"; - za podatke čijim bi otkrivanjem mogle nastupiti teže štetne posledice za bezbednost i interese Crne Gore
- "POVJERLJIVO"- za podatke čijim bi otkrivanjem mogle nastupiti štetne posledice za bezbjednost i interese Crne Gore

- "INTERNO"- za podatke čijim bi otkrivanjem nastupile štetne posledice za ostvarivanje funkcije organa

Ova četiri stepena tajnosti u skladu su sa međunarodnim standardima u ovoj oblasti.

Ono što, međutim predstavlja problem jeste što ovakav zakonodavni okvir ne daje jasna upustva u pogledu toga kako se sprovode testovi štetnosti i javnog interesa niti smernice u pogledu toga koje bi kategorije podataka mogle da nanesu štetne posledice za bezbednost i interese Crne Gore. U uporednim zakonodavstvima ovo pitanje se načelno rešava na nekoliko načina:

a) podatak koji se označava tajnim mora pripadati nekim širim kategorijama (temama) koje su izričito navedene u spisku koji predstavlja integralni deo samog propisa. Ovakva praksa je karakteristična za nekadašnje komunističke države, a cilj zakonodavca je da se izbegne prekomerna klasifikacija podataka. Primer za takvo rešenje predstavlja zakonodavstvo Estonije[28], gde su u samom tekstu zakona navedene vrste podataka koje se smatraju tajnim i odgovarajući stepen tajnosti – npr. podaci koji se odnose na lica i tajne agente koje su za potrebe tajne saradnje regrutovale agencije za nadzor smatraju se strogo poverljivim podacima.[29] Ovakvo zakonodavno rešenje nesumnjivo olakšava označavanje podataka tajnim, i, ukoliko je sistem dobro postavljen, mogućnosti za zloupotrebu su značajno sužene, dok su javnosti poznate kategorije tajnih podataka. Sa druge strane, postojanje previše ekstenizivnog spiska može dovesti do toga da lice ovlašćeno za označavanje spisak shvati previše doslovno, te da podatak označi tajnim samo zato što pripada nekoj od navedenih kategorija.

b) zakon ili podzakonski akt ukazuju ne na kategorije podataka, već konkretizuju interese za koje mogu nastati štetne posledice ako se podaci otkriju. Ovakva praksa postoji u regionu postoji u **Srbiji**, ali samo u odnosu na dva najviša stepena tajnosti – "državna tajna" i "strogo poverljivo" na nivou cele republike[30], dok se bliži kriterijumi za određivanje stepena tajnosti "poverljivo" i "interno" određuju na više nivoa – organa javne vlasti, ali odvojeno bezbedonosno-informativne

[28] Riigisaladuse ja salastatud välisteabe seadus Vastu võetud 25.01.2007, RT I 2007, 16, 77 dostupan na https://www.riigiteataja.ee/akt/105052017005, prevod dostupan na https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/519062017007/consolide
[29] Vid. Estonski zakon, član 8, stav 2.
[30] Uredba o bližim kriterijumima za određivanje stepena tajnosti "DRŽAVNA TAJNA" i "STROGO POVERLJIVO" Republike Srbije

agencije.[31] Primera radi, Uredbom o bližim kriterijumima za određivanje stepena tajnosti bliže se određuju kriterijumi za označavanje tajnosti na primer podatak se može označiti stepenom tajnosti "državna tajna" ako bi njegovim otkrivanjem neovlašćenom licu, njegovom zloupotrebom ili uništavanjem nastala neotklonjiva teška šteta po interese Republike Srbije, koja može imati neku od taksativno navedenih posledica, kao što su "neposredno i izuzetno ozbiljno ugrožavanje teritorijalnog integriteta i suverenosti, masovan gubitak ljudskih života ili izuzetno ozbiljnu pretnju po život i zdravlje ljudi, izuzetno ozbiljno ugrožavanje nacionalne i javne bezbednosti, odbrane ili aktivnosti bezbednosnih i obaveštajnih službi.[32]. Problem sa ovakvim načinom regulisanja je dvojak:

1. Regulisanje putem uredbe podložno je čestim izmenama i ne pruža dovoljno garantija u pogledu javnosti postupka u kome je regulatorno rešenje usvojeno. Osim toga, takođe postoji i mogućnost da se uredbom na neodgovarajući način proširi obuhvat podataka ili kategorija podataka koje treba označiti tajnim. Ujedno se time stvara novi rizik od neusklađenosti podzakonskog akta sa drugim propisima kojima se reguliše pristup informacijama od javnog značaja i zaštita podataka o ličnosti.

2. Ukazivanje na moguće štetne posledice svakako je korisna, ali ne i dovoljna smernica za sprovođenje testa štetnosti. Konkretno, u Uredbi koja je na snazi u Srbiji kategorije mogućih posledica i dalje su postavljene prilično široko i neodređeno. To za posledicu može imati široko tumačenje kriterijuma za označavanje podatka kao tajnog.

c) detaljno ukazivanjem na zaštićeni interes kategorije podataka i vrste posledica koje mogu nastupiti za zaštićene interese, te stepen tajnosti, u aktu koji nije pravno obavezujući, već predstavlja "meko pravo". Odličan primer ovakve prakse predstavljaju smernice koje je sačinila Vlada Australije.[33] Smernice istovremeno omogućavaju lakše praćenje gradacije štetnosti posledica i konkretizacije štetne posledice, te njihovo svrstavanje u odgovarajući stepen tajnosti, na primer:

[31] Uredba o bližim kriterijumima za određivanje stepena tajnosti „POVERLJIVO“ i „INTERNO“ u organima javne vlasti.
[32] Član 3. Uredbe.
[33] https://www.protectivesecurity.gov.au/governance/security-risk-management/Pages/Business-impact-levels.aspx

1 (nizak-srednji)	2 (Visok)	3 (Veoma visok)	4 (Izrazito visok)	5 (Katastrofalan)
Uticaj na odbrambene operacije				
Za posledicu ima ograničenu štetu za neoperativnu delotvornost ili bezbednost odbramenih snaga Australije ili saveznika bez rizika po život	Za posledicu ima štetu za neoperativnu delotvornost ili bezbednost odbrambenih snaga Australije ili saveznika što uzrokuje probleme u ponovnom snabdevanju koji mogu biti rizik po život	Za posledicu ima ograničenu štetu za operativnu delotvornost ili bezbednost odbramenih snaga Australije ili saveznika što može predstavljati rizik po život	Za posledicu ima ozbiljno oštećene operativne delotvnornosti ili bezbednosti odbrambenih snaga Australije ili saveznika.	Za posledicu ima izuzetno ozbiljnu štetu causing exceptionally grave damage to the operational effectiveness or security of Australian or allied forces

Šta bi bilo optimalno rešenje za Crnu Goru?

Postoje dve mogućnosti:

1. Promena zakonskog teksta tako da se već u samom zakonu bliže urede kriterijumi za označavanje podataka različitih stepena tajnosti, uz usvajanje smernica kojima bi se ukazalo na kategorije podataka koje se mogu označiti tajnim i/ili njihove štetne posledice, sledeći praksu Estonije ili Australije

2. Usvajanje podzakonskog akta ili smernica kojima će se bliže urediti kriterijumi za označavanje podataka različitim stepenima tajnosti, ukazivanjem na kategorije podataka koje se mogu označiti tajnim, na način na koji je to učinjeno u Estoniji, ili na njihove štetne posledice po zaštićene interese, na način na koji je to učinjeno u Australiji.

Smernice u vezi sa kategorijama podataka u vezi sa kojima se može ograničiti pristup bilo bi dobro uzeti iz Tšvane principa[34] prema kojima su to:

a) informacije o tekućim planovima, operacijama i kapacitetima dok je takav podatak u operativnoj upotrebi;

b) informacije o proizvodnji, sposobnostima ili upotrebi sistema naoružanja ili drugih vojnih sistema, uključujući i sisteme za komunikaciju;

c) informacije o posebnim merama za zaštitu državne teritorije, kritične infrastrukture ili nacionalnih institucija, usmerenih protiv pretnji, upotrebe sile ili sabotaže, čija delotvornost je uslovljena tajnošću;

d) informacija koja je deo, ili izvedena iz, operativnih radnji, izvora i metoda tajnih službi, dokle god se tiču pitanja nacionalne bezbednosti; i

e) informacije u vezi sa pitanjima nacionalne bezbednosti dostavljene od strane države ili međudržavnog tela kada se podrazumeva garantovanje režima poverljivosti, i ostale diplomatske komunikacije dokle god se tiču pitanja nacionalne bezbednosti.

Regulatorno rešenje koje je na snazi u Estoniji čini se previše detaljnim za zakonski tekst, ali svakako predstavlja dobru smernicu u pogledu toga kako se mogu bliže odrediti kategorije informacija koje se mogu označiti nekim stepenom tajnosti.

U vezi sa regulatornim okvirom Crne Gore potrebno je ukazati na još jedan praktičan izazov do koga dovodi međusobna neusklađenost Zakona o slobodnom pristupu informacijama od javnog značaja i Zakona o tajnosti podataka.

Naime, Zakonom o tajnosti podataka kao najniži stepen tajnosti propisana je oznaka "interno" za podatke čijim bi otkrivanjem nastupile štetne posledice za ostvarivanje funkcije organa. Ovi podaci, podsetimo, morali bi biti samo oni čijim bi otkrivanjem nepozvanom licu nastupile ili

[34] The Global Principles on National Security and the Right to Information (Tshwane Principles), https://www.opensocietyfoundations.org/sites/default/files/global-principles-national-security-10232013.pdf, princip 10

mogle nastupiti štetne posledice za bezbednost i odbranu, spoljnu, monetarnu i ekonomsku politiku Crne Gore. Istovremeno, Zakon o slobodnom pristupu informacijama od javnog značaja predviđa da se pristup informacijama od javnog značaja može uskratiti, između ostalog, ako je to

- u interesu prevencije, istrage i gonjenja učinilaca krivičnih dela, kako bi se zaštitili podaci koji se odnose na sadržinu preduzetih radnji u pretkrivičnom i krivičnom postupku, dokaze prikupljene uviđajem i istragom, mere tajnog nadzora, zaštićenog svedoka i svedoka saradnika, kao i efikasnost vođenja postupka,

- radi zaštite službene dužnosti u odnosu na podatke koji se odnose na planiranje inspekcijske kontrole i nadzora, konsultacije između i unutar organa vlasti u vezi sa utvrđivanjem stavova radi izrade službenih dokumenata i predlaganja rešenja nekog predmeta, rad i odlučivanje kolegijalnih organa, pokretanje i vođenje disciplinskog postupka.

Navedeni razlozi za uskraćivanje pristupa informacijama od javnog značaja nesumnjivo se mogu smatrati podacima čjim bi otkrivanjem nepozvanom licu nastupile ili mogle nastupiti štetne posledice za ostvarivanje funkcije organa zaduženih za bezbednost i odbranu. Ovakvo normiranje zapravo znači da je pred lice koje treba da odredi tajnost podatka postavljen vrlo osetiljiv zadatak sprovođenja testa štetnosti i testa javnog interesa u situacijama koje su međusobno veoma bliske te da proceni da li podatak treba označiti tajnim i odrediti mu stepen tajnosti "interno" ili na zahtev tražioca informacije od javnog značaja uskratiti pristup podacima po osnovu Zakona o slobodnom pristupu informacijama od javnog značaja, takođe nakon sprovođenja odgovarajućeg testa štetnosti i testa javnog interesa. U praksi to nadalje znači da će **neretko doći do prekomerne upotrebe oznake stepenat tajnosti "interno"**, naročito ako se ima u vidu i relativno širok krug lica koji podatak mogu označiti tajnim – podsetimo, to su starešine organa iz član državnih organa, organa državne uprave, organa jedinica lokalne samouprave i drugih pravnih lica kojima je povereno vršenje javnih ovlašćenja ili lica koji oni ovlaste. Ujedno, osnovi za označavanje nekog podatka tajnim postavljeni su prilično široko, i lako može doći do situacije u kojoj će se podaci koji se odnose na privatizaciju ili dnevno poslovanje privredih subjekata koji su u većinskom vlasništvu države proglasiti tajnim u cilju zaštite ekonomskih interesa. U tom smislu neophodno je ukazati na formulaciju koja je sadržana u samom zakonu a koja je ujedno i standard iz Evropske konvencije o ljudskim pravima a to je da ova ograničenja moraju biti "neophodna u demokratskom društvu". Otuda kroz podzakonske akte i izvore "mekog prava" treba dati dodatne smernice u

pogledu razgraničenja između potrebe da se neki podatak označi tajnim i potrebe da se pristup nekoj informaciji ograniči.

3. TRAJANJE OGRANIČENJA I TAJNOSTI PODATAKA

U kontekstu međusobnog usklađivanja, ali i unapređivanja Zakona o slobodnom pristupu informacijama i Zakona o tajnosti podataka potrebno je ukazati i na trajanje ograničenja pristupu informacijama, trajanje oznake tajnosti i njeno periodično preispitivanje.

Što se tiče Zakona o slobodnom pristupu informacijama, njegovim članom 15. propisana je dužina trajanja ograničenja pristupa informaciji, i to na sledeći način:

- zaštita privatnosti i informacija koja sadrži podatke o zaštićenom svedoku i svedoku saradniku – 70 godina od nastanka i najmanje 20 godina od smrti lica na koje se odnosi

- ograničenja radi bezbednosti, odbrane, spoljne, monetarne politike – do isteka rokova koji su propisani zakonom kojim se uređuje tajnost podataka.

- radi prevencije, istrage i gonjenja izvršilaca krivičnih dela – najduže do okončanja postupka

- radi vršenja službene dužnosti – do izrade službenog dokumenta ili utvrđivanja predloga rešenja nekog predemta, verifikacije zapisnika sa sednice kolegijalnog organa ili okončanja disciplinskog postupka

- radi zaštite trgovinskih i drugih ekonomskih interesa – do isteka roka u skladu sa zakonom kojim se uređuju prava intelektualne svojine.

Nema nikakvih odrednica u pogledu toga do kada se može ograničiti pristup podacima koji predstavljaju poresku tajnu te bi ciljno tumačenje moralo da uputi na odredbe Zakona o poreskoj administraciji, koje, međutim, ne ukazuje na to koliko dugo se poreska tajna čuva. Isto važi i za poslovnu tajnu.

Što se tiče vremena trajanja ograničenja pristupu informacijama, nije sasvim jasno zbog čega je propisan bilo kakav rok za ograničenje pristupa, budući da se pristup podacima ograničava na osnovu konkretnog zahteva konkretnog podnosioca. Možda je namera zakonodavca bila da na ovaj

način ukaže organima javne vlasti na to da o zaštiti pojedinih kategorija podataka treba da vode računa i prilikom proaktivnog pristupa informacijama od javnog značaja,i jedino u tom slučaju se može razumeti norma ovakve sadržine. U suprotnom, to bi značilo da će organ tražiocu "automatski" odbiti pristup informaciji od javnog načaja pozivajući se na rok trajanja ograničenja. Ovakva praksa bi se morala obeshrabriti.

Ono što predstavlja dodatni problem jeste i način na koji su rokovi određeni – na primer, okončanje postupka u slučaju zaštite istrage i gonjenja izvršilaca krivičnih dela – da li se misli na okončanje konkretne faze postupka ili celokupnog krivičnog postupka pravnosnažnom presudom? U potonjem slučaju može doći do apsurdne situacije u kojoj bi se ograničavao pristup informacijima koje su već učinjene javnim u sudskom postupku i javnoj prvostepenoj presudi. Otuda bi bilo **dobro ovaj član zakona u potpunosti brisati, a rokove tokom kojih je potrebno čuvati tajnost pojedinih podataka jasno propisati odgovarajućim propisom, odnosno Zakonom o poreskoj adminstraciji i slično.**

Što ste tiče dužine trajanja tajnosti podataka prema Zakonu o tajnosti podataka, ovu dužinu označava lice koje je ovlašćeno da podatak označi tajnim, ili, ako ono to ne učini, onda se primenjuju zakonom propisani rokovi, a to su:

1) 30 godina - za podatke označene stepenom tajnosti "STROGO TAJNO";
2) 15 godina - za podatke označene stepenom tajnosti "TAJNO";
3) pet godina - za podatke označene stepenom tajnosti "POVJERLJIVO";
4) dve godine - za podatke označene stepenom tajnosti "INTERNO.[35]

Treba napomenuti da lice koje podatak označava tajnim ne može odrediti prestanak tajnosti u roku koji je duži od gore pomenutih rokova propisanih zakonom. Sa druge strane, Zakonom je takođe propisano da, izuzetno, ovlašćeno lice za određivanje stepena tajnosti podatka može produžiti rok tajnosti podatka, ako prije isteka roka iz stava 1 ovog člana utvrdi da postoje razlozi koji se tiču bezbjednosti, i to najduže za vremenski period propisan za pojedine stepene tajnosti iz stava 1 ovog člana. To praktično znači da se trajanje oznake tajnosti može višestruko produžiti, budući da Zakonom nije propisano nikakvo ograničenje broja ovakvih produženja. Ovakvo rešenje se čini naročito neopravdanim u slučaju oznake stepena tajnosti "interno" koja, podsetimo, služi

[35] Član 19a, stav 1 Zakona.

da zaštiti "ostvarivanje funkcije organa". Ipak, Direkcija za tajnost podataka usvojila je stav da se rok tajnosti može maksimalno produžiti za zbirno isti broj godina na koji je prvi put označen, bez obzira koliko puta se rok produžavao.[36] Ipak, bilo bi **uputno da se ovaj stav unese u zakonski tekst ili barem u tekst nekog podzakonskog akta.**

Zakonom o tajnosti podataka[37] propisana je i obaveza periodičnog preispitivanja oznake tajnosti, prilikom koje se oznaka tajnosti može promeniti ili ukinuti. Periodično preispitivanje obavlja Komisija koju imenuje starešina organa i to:

1) podatke označene stepenom tajnosti "STROGO TAJNO", najmanje jednom u tri godine;

2) podatke označene stepenom tajnosti "TAJNO", najmanje jednom u tri godine;

3) podatke označene stepenom tajnosti "POVJERLJIVO", najmanje jednom u tri godine;

4) podatke označene stepenom tajnosti "INTERNO", najmanje jednom godišnje

Ako se ima u vidu dužina trajanja oznake tajnosti, čini se da su periodi u kojima je vrši periodično preispitivanje oznaka tajnosti "POVJERLJIVO" I "INTERNO" postavljeni prilično dugačko i da bi bilo uputno skratiti ih. Ipak, uvođenje vanrednog preispitivanja u slučaju kada se zahteva pristup tajnom podatku predstavljao bi dodatnu korektivnu meru u tom pogledu, kao što je istaknuto ranije u tekstu. Upućujemo u tom pogledu na hrvatski Zakon o tajnosti podataka[38] čijim članom 16 je propisano da kada postoji interes javnosti, vlasnik podatka je dužan da oceni ravnotežu između prava na pristup informacijama i zaštite vrednosti propisanih Zakonom o tajnosti, koje se tajnošću i šitte, te odlučiti o zadržavanju tajnosti, promeni stepena tajnosti, deklasifikaciji ili oslobađanju od obaveze čuvanja tajnosti podatka. Hrvatski zakon takođe porpisuje da pre donošenja ovakve odluke, vlasnik podatka mora da zatraži mišljenje kancelarije Vijeća za nacionalnu sigurnost.

4. JAVNE NABAVKE I TAJNOST I POVERLJIVOST PODATAKA

[36] "Transparentnost i odbrana u Crnoj Gori", str. 20
[37] Član 19b
[38] NN 79/07, 86/12

Zakonom o javnim nabavkama[39] je propisano da se on ne primenjuje na nabavke iz oblasti odbrane i bezbednosti koje sadrže elemente iz čl. 175, 176 i 177 tog zakona, dakle, koje ispunjavaju određene uslove. U ovom delu ćemo se kratko osvrnuti na pitanje tajnosti podataka u vezi sa javnim nabavkama u sektoru odbrane.

Predmet javne nabavke u oblasti odbrane i bezbjednosti, u smislu ovog zakona, su:

1) vojna oprema, sa svim djelovima, komponentama ili podsklopovima;

2) bezbjednosno osjetljiva oprema, sa svim djelovima, komponentama ili podsklopovima;

3) roba, usluge i radovi koji su direktno povezani sa opremom iz tač. 1 i 2 ovog stava, u toku čitavog ili dijela životnog ciklusa;

4) usluge i radove samo za vojne namjene;

5) bezbjednosno osjetljive usluge.

Listu vojne opreme i proizvoda iz stava 1 ovog člana propisuje Vlada.

Posebne javne nabavke u oblasti odbrane i bezbjednosti su nabavke:

1) koje su uređene posebnim propisima o nabavkama, u skladu sa međunarodnim sporazumom ili ugovorom zaključenim između Crne Gore i jedne ili više država;

2) koje su uređene posebnim propisima o nabavkama, u skladu sa međunarodnim sporazumom ili ugovorom koji se odnosi na stacioniranje trupa i odnose se na privredna društva registrovana u Crnoj Gori, državi članici Evropske unije ili drugoj državi, koja učestvuju u postupku javne nabavke;

3) koje je Crna Gora dužna da dodijeli u skladu sa posebnim pravilima međunarodne organizacije;

4) kod kojih bi primjena odredbi ovog zakona obavezala Crnu Goru da pruži informacije čije otkrivanje je u suprotnosti sa vitalnim interesima njene bezbjednosti;

5) u svrhe obavještajnih aktivnosti;

[39] 74/2019

6) u okviru programa saradnje zasnovanih na istraživanju i razvoju novog proizvoda koji zajednički sprovode Crna Gora i najmanje jedna država članica Evropske unije i, kada je potrebno, za kasnije faze čitavog ili dijela životnog ciklusa tog proizvoda;

7) dodijeljene u trećoj državi, uključujući i one za civilne svrhe, gdje su snage raspoređene izvan teritorije Evropske unije, ako operativne potrebe zahtijevaju da se ugovori zaključe sa privrednim subjektima koji se nalaze u zoni operacija;

8) koje sprovode državni organi Crne Gore sa državnim organima država članica Evropske unije ili treće države, a odnose se na:

a) nabavku vojne opreme ili sigurnosno osjetljive opreme;

b) radove i usluge direktno povezane sa opremom iz podtačke a ove tačke; ili

c) radove i usluge za izričito vojne namjene ili sigurnosno osjetljive radove i sigurnosno osjetljive usluge;

9) ako se zaštita bitnih bezbjednosnih interesa Crne Gore ne može obezbijediti određivanjem zahtjeva u cilju zaštite tajnosti podataka koje naručilac stavlja na raspolaganje ponuđačima na način propisan ovim zakonom;

10) koje su proglašene tajnim ili koje moraju biti propraćene posebnim bezbjednosnim mjerama u skladu sa zakonom ili aktom nadležnog organa ili se odnose na bezbjednost štićenih lica Crne Gore, pod uslovom da je Crna Gora utvrdila da bitne bezbjednosne mjere i interese nije moguće zaštiti mjerama iz tačke 9 ovog člana;

11) roba i usluga iz člana 175 ovog zakona čija je procijenjena vrijednost jednaka ili manja od 20.000,00 eura, odnosno radova čija je procijenjena vrijednost jednaka ili manja od 40.000,00 eura.

Postojanje ovakve vrste nabavki nije u neskladu sa relevantnim međunarodnim standardima. Istovremeno, njihovo određenje nije značajno drugačije od zakonskog određenja ove kategorije predmeta u prethodnom crnogorskom zakonu o javnim nabavkama. Unapređenje predstavlja nešto

detaljnija Uredba kojim se propisuju pravila postupka sprovođenja javnih nabavki u bezbednosnom sektoru.

Opravdano se postavlja pitanje u kakvom odnosu mogu biti nabavke u oblasti odbrane i bezbednosti, propisi o tajnosti podataka i propisi o slobodnom pristupu informacijama od javnog značaja. Ovo je naročito značajno ako se uzme u obzir da su ove nabavke i izuzete od opšteg režima s obzirom na to da su uglavnom radi o bezbednosno osetljivim podacima, to jest, da se propisivanjem posebnog postupka štite interesi bezbednosti države.

U tom pogledu kategorije "usluga i radova za isključivo vojne namene" predstavlja unekoliko široko postavljen izuzetak, budući da se pojam "vojne namene" ne definiše niti u zakonu o javnim nabavkama tako ni u Zakonu o vojsci.[40]

Vlada Crne Gore je 2020. godine usvojila Uredbu o Listi vojne opreme i proizvoda, postupku i načinu sprovođenja javnih nabavki u oblasti odbrane i bezbjednosti.[41] Ova Uredba sadrži dva priloga – samu listu vojne opreme i proizvoda, koja je u određenim delovima i dalje prilično široko formulisana (npr. pod tačkom 11 predviđeno je da vojnu opremu i proizvode čine „vojna i policijska elektronska oprema“), kao i odredbe o sprovođenju postupka bezbednosnih nabavki. Prilogom 1 detaljnije su propisana pravila o zaštiti klasifikovanih, odnosno tajnih podataka. Stavom 18 ukazuje se da, ako naručilac tokom postupka bezbednosne nabavke namerava da privrednim subjektima stavi na raspolaganje klasifikovane podatke, on je dužan da odredi dokaze koji su privredni subjekti dužni da dostave radi zaštite klasifikovanih podataka – to su podaci klasifikovani u sklad usa Zakonom o tajnosti podataka. Ako privredni subjekat ne dostavi traženu izjavu ili dozvolu, naručilac mu neće dozvoliti pristup. Ovakvo ograničenje može se smatrati celishodnim. Ipak, Prilogom 1 predviđaju se i dodatna pravila, kojima se omogućava dalje ograničavanje pristupa informacijama o nabavkama u oblasti bezbednosti. Naime, njime se načelno predviđa da naručilac može da uskrati određene informacije koje se tiču zaključivanja ugovora o bezbjednosnoj nabavci, klasifikovanog ugovora ili okvirnog sporazuma, ako bi njihovo objavljivanje bilo suprotno odredbama posebnog zakona ili protivno javnom interesu, naročito interesu odbrane i bezbjednosti, ako bi štetila opravdanim poslovnim interesima privrednih subjekata ili bi mogla štetiti fer tržišnom nadmetanju između tih subjekata. Nije do

[40] Sl. list CG, br. 51/2017 i 34/2019
[41] Sl. List CG br. 76/2020

kraja jasno u kom trenutku i sa kojim ciljem se ove informacije uskraćuju, te bi ovo pravilo bilo neophodno dodatno razraditi. Napominjemo da su gotovo istovetne odredbe prisutne u pravnom okviru u regionu, na primer, u Uredbi o javnoj nabavi u području obrane i sigurnosti Republike Hrvatske.[42] Sam klasifikovani ugovor u Prilogu 1 određen je isti način kao i u hrvatskom zakonodavstvu, kao ugovor zaključen u pisanom obliku između jednog ili više ponuđača i jednog ili više naručilaca, čiji je predmet nabavke izvođenje radova, isporuka robe ili pružanje usluga, a koji sadrži klasifikovane podatke ili čije sprovođenje zahtijeva pristup klasifikovanim podacima. Prilog 1 ne sadrži nikakve dalje odredbe o klasifikovanim ugovorima te ostaje nejasan eventualni posebni pravni režim koji bi se imao na njih primeniti, kao ni odnos između ovog propisa i propisa o slobodnom pristupu informacijama. Potrebno je stoga pravni režim klasifikovanog ugovora bolje regulisati i jasnije referisati na odnos sa pravnim režimima za tajnost podataka i slobodan pristup informacijama. Ovako, pravni okvir ostaje nedorečen.

Zanimljiva je i odredba Priloga 1 koja se odnosi na objavljivanje obaveštenja o zaključenom ugovoru o bezbednosnoj nabavci ili okvirnom sporazumu. Njome[43] je propisa da je naručilac obavezan da obaveštenje o zaključenom ugovoru o bezbjednosnoj nabavci ili okvirnom sporazumu objavi u roku od **48** dana od dana zaključivanja ugovora ili okvirnog sporazuma. To predstavlja značajno odstupanje od opštih odredbi Zakona, prema kojima je naručilac dužan da odluku o izboru najpovoljnije ponude objavi u roku od 3 dana od dana donošenja, a ako su pojedini podaci iz odluke tajni u skladu sa zakonom kojim se uređuje tajnost podataka, odluka će se objaviti na način kojim će se ti podaci na odgovarajući način zaštititi.

Zakonom[44] je propisano da naručilac može, tenderskom dokumentacijom, da odredi tajnim određene podatke koje privrednim subjektima stavlja na raspolaganje u postupku javne nabavke, u skladu sa zakonom kojim se uređuje tajnost podataka. Ovakvo regulisanje ne čini se celishodnim. Sa jedne strane, čini se da je zakonodavac učinio napor da označavanje nekog podatka kao tajnog podvede pod opšti režim tajnosti podataka, što je načelno ispravna intencija. Istovremeno, podsetimo da se podaci označavaju kao tajni ukoliko bi njihovo otkrivanje prouzrokovalo štetu za zaštićene interese, a to su bezbednost Crne Gore, spoljna, ekonomska i monetarna politika. Ova

[42] NN 19/2018
[43] Stav 34 Priloga
[44] Član 30 Zakona o javnim nabavkama

norma ne predstavlja unapređenje u odnosu na režim koji je bio predviđen prethodnim zakonom, i može izazvati dodatnu konfuziju. Na samom početku, jezičko tumačenje ove norme ukazivalo bi na to da se ne radi o podacima koji su već označeni nekom od oznaka tajnosti, već da se prilikom tenderskog postupka označavaju kao tajni – što nipošto ne može predstavljati dobro rešenje, čak i kada bi klasifikacija ovih podataka predstavljala zaštitu zakonom propisanih interesa.

Lakše je zamisliti situaciju u kojoj bi pojedini tenderski podaci predstavljali poslovnu tajnu u smislu odredbi Zakona o privrednim društvima ili drugog propisa. U tom slučaju bi bilo **uputno da se u u posebnom zakonu odrediti pojam poslovne tajne i jasno urediti uslove pristupa i režim poverljivosti poslovne tajne te zaštite poslovne tajne, sa jasnim određivanjem odnosa tog zakona sa zakonom kojim se reguliše tajnost podataka i pristup informacijama od javnog značaja.**

Na osnovu svega prethodno iznetog jasno je da ni novousvojeni režim koji se odnosi na javne nabavke i nabavke u oblasti odbrane i bezbednosti ne predstavlja optimalno rešenje, niti postavlja odgovarajući balans između prava javnosti da zna i legitimne potrebe zaštite interesa odbrane i bezbednosti. Nedavno sprovedeno istraživanje[45] pokazuje da sistem planiranja i izveštavanja o bezbednosnim nabavkama nije bitno unapređen, te da ostaje uglavnom nepoznanica za javnost. Otuda se čini da je i ovaj, novi pravni okvir potrebno revidirati.

[45] https://institut-alternativa.org/licna-karta-nabavki-u-sektoru-bezbjednosti-i-odbrane/, pristup 19.5.2021.