Osobni podaci, tajni podaci i pristup novinara informacijama

*Alen Rajko**

UDK 342.738
342.732
Stručni rad
Primljeno: 20. 11. 2000.
Prihvaćeno: 20. 12. 2000.

U radu se analiziraju pravne situacije do kojih dolazi u okviru relacija između triju pitanja: tajnosti podataka, zaštite osobnih podataka i prava novinara na pristup informaciji. Iznijete su i osnovne odrednice aktualne radne verzije Nacrta prijedloga zakona o zaštiti osobnih podataka. Predlažu se mjerila rješavanja sukoba između pravom zaštićenih interesa povezanih sa spomenutim pitanjima.

Ključne riječi: osobni podaci, tajni podaci, pristup informaciji

1. Uvod

Zamislimo sljedeću situaciju. Građanin X ima informaciju da je osoba Y zaposlena kao srednjoškolski profesor na temelju krivotvorene diplome i rodnog lista. O tome je obavijestio nadležna prosvjetna tijela, koja međutim nisu reagirala. Potom je od škole u kojoj Y radi zatražio uvid u spornu diplomu ili domovnicu kako bi njihovu vjerodostojnost mogao provjeriti kod navodnih izdavatelja tih dokumenata. Škola odbija zahtjev, pozivom na propise o zaštiti osobnih podataka i o razgledanju spisa u upravnom postupku. X se obraća matičnom uredu, tražeći uvid u spis upisa u maticu rođenih. Matični ured odbija zahtjev, navodeći, osim već spomenutih, dodatni razlog: X nije legitimiran niti po propisima o državnim maticama.

* Mr. sc. Alen Rajko, načelnik Sektora kadrovskih, pravnih i obrazovnih poslova Policijske uprave primorsko-goranske, Rijeka.

Uvođenjem dodatnih elemenata opisana se situacija (barem pravno) mijenja. Primjerice, što se zbiva ako građanin X svoja saznanja ispriča novinaru, koji u odnosu prema navedenim tijelima raspolaže pravom pristupa informaciji, ali i mogućnošću prijetnje najavom objavljivanja priče s njihovom suradnom ili bez nje? Novinari nemaju pravo pristupa državnim i vojnim tajnama, što spomenuti podaci nisu. Situacija se, međutim, ponovno mijenja ako Y nije zaposlen kao srednjoškolski profesor, nego kao vojni službenik, a ministar obrane može podzakonskim aktom podatke o vojnom osoblju proglasiti vojnom tajnom.

Vratimo se početnom primjeru: podaci o Y nisu ni državna ni vojna tajna, ali je pristup novinarima ograničen propisima o zaštiti osobnih podataka. Mijenja li se pravna situacija ako je Y zaposlen kao zamjenik ministra prosvjete, što ga nedvojbeno čini javnom osobom? Ako se mijenja, na kojoj razini prestaje smanjeni opseg zaštite osobnosti javnih osoba - ulazi li u te okvire, primjerice, ravnatelj srednje škole. Ili, u drugome (vojnom) primjeru, ako Y nije obični vojni službenik, već npr. zamjenik ministra obrane: preteže li zaštita njegovih podataka pozivom na vojnu tajnu ili interes javnosti da zna je li visoki dužnosnik krivotvorio svoje dokumente, odnosno slijedom činjenice da se radi o javnoj osobi, što njezine osobne podatke čini u određenoj mjeri dostupnijima?

Navedeni primjeri ilustriraju važnost raščlanjivanja relacija između triju pitanja:

a) tajnosti podataka;

b) zaštite osobnosti (s naglaskom na osobnim podacima);

c) prava novinara na pristup informaciji.

Svako od tih pitanja i samo za sebe može postati poprište sukoba jakih i suprotstavljenih interesa. U slučajevima njihova djelomičnog preklapanja zbiljski se sukob potencira, a pravna se situacija komplicira.

Rad se prvenstveno odnosi na podatke u posjedu tijela javne vlasti (*arcana imperii* - "tajne vladajućih").

Pokušat ćemo skicirati početnu shemu razmatranja:

1. podaci su dostupni, osim u slučajevima kada su proglašeni povjerljivima[1] (na temelju propisa o tajnosti podataka odnosno o zaštiti osobnih podataka);

[1] Za novinare vrijedi predmnjeva dostupnosti informacija (uz negativnu enumeraciju iznimaka), dok je pravo ostalih subjekata na pristup informaciji posebno regulirano različitim propisima, prvenstveno postupovnim propisima,

2. novinarima je dostupan i dio povjerljivih podataka;
3. novinari nisu dužni otkriti izvor informacije, što ojačava njihov stvarni položaj u pristupu tajnim i(li) osobnim podacima;
4. ostvarivanje pristupa podacima putem javnosti sudbenoga i upravnog postupka te putem uvida u spis predmeta posebno je uređeno odgovarajućim postupovnim zakonima;
5. osobnost javnih osoba uživa manji stupanj pravne zaštite;
6. pojedini podaci mogu biti "dvostruko" zaštićeni: i prema propisima o tajnosti podataka i prema propisima o zaštiti osobnih podataka;
7. javljaju se tri glavne vrste subjekata s legitimnim interesima: građani, javna vlast i novinari;
8. javni interes dužna je štititi i javna vlast (zaštitom zakonito i opravdano zaštićenih podataka) i novinari (osiguravajući da javnost bude upoznata sa svim javno relevantnim podacima);
9. građanin ima pravo na zaštitu svojih osobnih podataka (pri čemu javna vlast ima pozitivnu obvezu da osigura tu zaštitu, a novinari negativnu obvezu poštovanja privatnosti), ali istodobno i pravo da bude (barem putem novinara) upoznat sa svim podacima od javne važnosti (osim zakonito i opravdano klasificiranih podataka);
10. kako se radi o materiji koja se dijelom odnosi na sukob pravno zaštićenih interesa, u određenim situacijama javlja se potreba da se posegne za testom pretežnosti interesa: pravo znati, pravo na zaštitu osobnih podataka i pravo na slobodu mišljenja i izražavanja nisu apsolutna prava.

2. Pravna i zbiljska situacija - opće naznake

Najprije na razini osnovnih informacija iznosimo glavne pravne elemente analize odnosa tajnosti, osobnih podataka i prava novinarskog pristupa informacijama (okvir određen ustavnim odredbama te međunarodnim ugovorima i zakonima), a potom i osnovne naznake stvarne situacije. Svako

propisima s područja sustava državne uprave te propisima kojima se uređuje uporaba pojedinih podataka (npr. propisi o arhivima, posvojenju, maticama, kaznenoj evidenciji i dr.). Opširnije o različitom položaju pojedinih subjekata u pristupu informacijama u nastavku rada.

od triju spomenutih pitanja bit će ukratko posebno razmotreno u idućem poglavlju.

2.1. Pravna razina

Na ustavnoj razini, zajamčeno je štovanje i pravna zaštita osobnoga i obiteljskog života, dostojanstva, ugleda i časti (čl. 35. Ustava Republike Hrvatske - u nastavku: Ustav[2]) te sigurnost i tajnost osobnih podataka (čl. 37). U okviru prava na slobodu mišljenja i izražavanja misli novinarima je zajamčeno pravo pristupa informaciji (čl. 38. st. 3). Zakonskom reguliranju prepušteni su zaštita podataka i nadzor nad radom informatičkih sustava u zemlji (čl. 37. st. 2. Ustava).

Pravo na poštovanje privatnoga i obiteljskog života zajamčeno je i u čl. 8. Europske konvencije za zaštitu ljudskih prava i temeljnih sloboda (u nastavku: Europska konvencija[3]), koja čini dio unutarnjega pravnog poretka Republike Hrvatske. U čl. 10. Europske konvencije određeno je pravo na slobodu izražavanja i informiranja, što uključuje slobodu mišljenja i slobodu primanja i širenja informacija i ideja bez miješanja javne vlasti i bez obzira na granice[4]. Obje odredbe sadrže i ograničenja prava, među kojima i ona bitna za temu ovog rada: državna sigurnost, javni red i mir, zaštita zdravlja ili morala (čl. 8. st. 2. i čl. 10. st. 2), odnosno zaštita prava drugih (čl. 8. st. 2), zaštita ugleda ili prava drugih, sprečavanje odavanja povjerljivih informacija (čl. 10. st. 2).[5]

Ustavno pravo novinara na pristup informaciji razrađeno je u čl. 5. Zakona o javnom priopćavanju (u nastavku: ZJP[6]). Slijedom odredbe čl. 37. st. 2. Ustava donijet je Zakon o zaštiti tajnosti podataka (u nastavku: ZZTP[7]), kojim su propisani pojam, vrste i stupnjevi tajnosti te mjere i postupci utvrđivanja, uporabe i zaštite tajnih podataka. Od triju navedenih pitanja na razini zakona najveća praznina postoji u pogledu zaštite osobnih podataka

[2] NN 8/98 i 113/00

[3] NN MU 18/97

[4] Spomenuta prava zajamčena su i drugim međunarodnim dokumentima, npr.: čl. 12. Opće deklaracije o pravima čovjeka (1948), čl. 17. Međunarodnog pakta o građanskim i političkim pravima (1966) - poštovanje privatnoga i obiteljskog života; čl. 19. Opće deklaracije, čl. 19. Međunarodnog pakta - pravo na slobodu mišljenja i izražavanja.

[5] Navedena ograničenja moraju biti zakonski određena, imati legitimni cilj i biti nužna (za postizanje odnosnog cilja) u demokratskom društvu.

[6] NN 83/96 i 20/00

[7] NN 108/96

i nadzora nad radom informatičkih sustava (čl. 37. Ustava), dok je zaštita ostalih ključnih aspekata prava na osobnost, obuhvaćenih čl. 35. Ustava, uređena ponajprije odredbama kaznenoga, građanskog, policijskog i medijskog prava.

Sudjelovanje u Radnoj grupi za izradu radnog teksta Nacrta prijedloga zakona o zaštiti osobnih podataka (u nastavku: ZZOP) omogućuje nam da u analizu uključimo barem osnovne konture buduće hrvatske regulacije zaštite osobnih podataka i nadzora nad informatičkim sustavima[8] (opširnije pod 3.2).

2.2. Razina zbilje

Koje su glavne karakteristike zbiljske situacije? Pojednostavljeno rečeno, i strana i domaća iskustva upućuju na zaključak da su metode rada te profil stvarnih i fiktivnih "klasičnih špijuna" danas u znatnoj mjeri postali nepotrebni. Nepažnja, trgovina informacijama, povlaštene veze, hakeri, prošireno područje medijske slobode i medijska kompetitivnost mijenjaju količinu dostupnih povjerljivih podataka, sankcije za povrede obveze povjerljivosti, brzinu pristupa podacima i ambijent njihova pribavljanja[9]. U hrvatskom slučaju tome treba pridodati još barem dva činitelja: "poplavu" informacija povezanu s prvom smjenom izborne većine nakon 1990. godine te još prije uhodanu praksu da se velik dio ključnih političkih događaja ne odvija neposredno u klasičnoj političkoj areni, već u medijskom prostoru[10]. Ne smijemo, pritom, zaboraviti niti predsjedničke stenograme, koji su već prerasli u zaseban političko-pravno-medijski fenomen.

S druge strane, sve je jednostavnije, a u stvarnosti i prisutnije, prikupljanje i obrada osobnih podataka, a time i mogućnost njihove zlorabe.

[8] Radi se o tekstu Nacrta usuglašenom u okviru Radne grupe u vrijeme pisanja ovog rada (studeni 2000. godine). Tekst će vjerojatno doživjeti određene preinake nakon primitka mišljenja eksperata Vijeća Europe i nadležnih hrvatskih ministarstava.

[9] Ograničavanje neopravdane tajnosti jača demokratski poredak. "Obilje" povjerljivih podataka ima međutim svoje naličje. Pritom se javljaju dva glavna rizika: *(1)* povreda legitimnih interesa koji su trebali biti zaštićeni tajnošću podataka (npr. kaznene istrage, osobni podaci); *(2)* namjesto tradicionalnoga državnog manipuliranja tajnošću, skriveno iza "široke dostupnosti podataka" sve je raširenije manipuliranje relevantnošću i kontekstom (kako od strane javnoga, tako i privatnog sektora).

[10] Široko je raširено mišljenje da su spomenutoj promjeni izborne većine više pridonijeli mediji (potpomognuti svojih nepresušnim kanalima pribavljanja kompromitirajućih podataka "iznutra") negoli politička oporba.

Izostavljajući ovom prilikom "standardne" oblike zaobilaženja tajnosti (poput špijunaže, hakerskih "provala" i dr.) i zlorabe osobnih podataka (država kao "veliki brat"), tipični slučajevi opisanoga "informacijskog propuha", s jedne, te manipuliranja osobnim podacima, s druge strane, mogu se ilustrirati u sljedećih nekoliko primjera.

Sindrom nestalih laptopa. Riječ je o kršenju standarda sigurnosti podataka zbog nemara. Laptope smo izabrali kao naziv te skupine primjera zbog njihovih učestalih nestanaka u vrijeme pisanja ovog rada (npr. krađa laptopa s podacima koji su opisani kao *više nego strogo povjerljivi* iz Ureda za obavještajne poslove *State Departmenta*; britanskim vladinim dužnosnicima od 1997. godine nestalo je i ukradeno 97 laptopa, uključujući nedavnu krađu laptopa ministra vojske Spellara). U tu se skupinu mogu svrstati i primjeri poput pogrešne elektroničke dostave povjerljivih dokumenata na "obične" web stranice (npr. slanje više tajnih poruka britanske Kraljevske ratne mornarice 15-godišnjoj djevojčici[11]; "pojavljivanje" bilješke o razgovorima američkih i japanskih obavještajaca).[12] Kao hrvatski primjer ove skupine slučajeva može poslužiti svojedobno nalaženje dokumenata Ministarstva obrane u kantama za smeće.

Mangupi u našim redovima. U srpnju 2000. godine britanski *Sun* objavio je povjerljivi memorandum savjetnika za ispitivanje javnosti prvog ministra Blaira, u kojem se, između ostalog, navodi da ministri nemaju dodira s potrebama birača, a Vlada nije ispunila predizborna obećanja o zdravstvenoj zaštiti i suzbijanju kriminala te joj nedostaju istinski patriotski osjećaji. Samo nekoliko tjedana prije duhove na Otoku (prije svega britanskih obavještajaca) uzburkala je najava prijašnje čelnice tajne službe *MI5* da će objaviti svoje memoare. Preuzimajući predsjedanje Europskom komisijom, Romano Prodi uveo je obvezatna pravila ponašanja, skup etičkih i političkih načela, koja obuhvaćaju i obvezu striktnog poštovanja kolegijalnosti i tajnosti u radu Komisije. To, među inim, znači da je zabranjen svaki komentar članova

[11] Među inim, poruke su se odnosile na: pritužbe na probleme u vezi komunikacijskom opremom na britanskim nosačima zrakoplova; sustav upravljanja osjetljivim podacima između Sjedinjenih Država, Ujedinjenog Kraljevstva, Australije, Novog Zelanda i Kanade; novu tehnološku strategiju ratne mornarice Novog Zelanda; posprdna imena i opise visokih časnika i službenika Ministarstva. K tome, Mornarica je ignorirala obavijest obitelji djevojčice o pristiglim podacima i nastavila ih slati još puna četiri mjeseca.

[12] *Jutarnji list*: 18.04.2000. (56. str.); 28.05.2000. (48. str.); 06.06.2000. (48. str.); 13.06.2000. (48. str.); 24.07.2000. (48. str.).

Komisije *koji bi dovodio u pitanje odluke Komisije* te da se moraju uzdržati od *otkrivanja sadržaja rasprava na Komisiji*. Od afere *Watergate* - neposredno na američkoj, a posredno na globalnoj razini, do redovitoga (u nastavcima) medijskog objavljivanja povjerljivih dokumenata u domaćem tisku - na hrvatskoj razini, potvrđuje se pravilo da osveta, trgovina (protu)uslugama, korupcija, eliminiranje takmaca ili želja za upozoravanje javnosti na nedopušteno u vlastitim redovima jamče "novačenje" dovoljnog broja "unutarnjih izvora".

Javnost kao saveznik. Podaci koji su (propisno i opravdano ili ne) proglašeni tajnima ponekad se objavljuju bez skrivanja. Tako je saborski zastupnik i član Odbora za unutarnju politiku i nacionalnu sigurnost Damir Kajin u srpnju 2000. godine javno ilustrirao teškoće u Ministarstvu obrane navođenjem navodno povjerljivih podataka o teškom stanju u Ministarstvu koje je čuo na zatvorenoj sjednici Odbora u Varaždinu, što je izazvalo kratkotrajne javne kontroverzije. U takvim slučajevima (ne)klasificiranost pojedinog podatka postaje sporedna. Dovoljno rašireno uvjerenje da se radi o podacima za koje građani (ako ni zbog čega drugog, kao birači, porezni i vojni obveznici) trebaju znati omogućuje "otkrivatelju" da nastupi transparentno i neposredno.

Fenomen klatna. Uravnoteženi pristup tajnosti podataka obuhvaća zakonito i opravdano klasificiranje, probitačne i odgovorne medije, senzibiliziranu javnost i razvijene demokratske institucije. Jedna od prepreka takvome uravnoteženom pristupu jest *fenomen klatna*: što se duže klatno drži u jednome od krajnjih položaja, njegovim otpuštanjem najprije odlazi u drugi krajnji položaj, a tek nakon određenog vremena zaustavlja se na sredini. Nedavna hrvatska iskustva i u ovom slučaju mogu poslužiti kao dobar primjer: klatno je otpušteno iz krajnjeg položaja mistificirane (ponekad i fetišizirane) tajnosti (položaja u kojem se nalazilo znatno duže od proteklog desetljeća). U razdoblju do zaustavljanja u srednjem položaju, gdje se susreću pravo znati i sigurnosna kultura, u javnosti neće nedostajati povjerljivih informacija.

Trgovci kao "veliki brat". Sve je manje ljudi iznenađeno kada na svoju kućnu adresu prime katalog tvrtke od koje prije nisu nikada naručivali robu. Trgovački lanci u novije doba postaju sve ozbiljnija prijetnja pravu na osobnost. Primjerice, američko Savezno povjerenstvo za trgovinu izrazilo je

zabrinutost i pokrenulo istragu o tvrtkama koje preko Interneta prikupljaju podatke o svojim kupcima, "ugrađujući" na njihova računala identifikacijske oznake. To omogućuje pojedinim tvrtkama da razmjenjuju informacije o kupcima, njihovim potrebama, navikama, novčanom stanju, pa čak i osobne podatke[13].

Mreža nadzornog profila. Samostalni informacijski sustavi, javni ili privatni, lako se povezuju u mrežu, iz koje se dobivaju potpuno nove formulacije podataka od onih koji su prvobitno prikupljeni. Najveća opasnost za pravo na osobnost jest konstrukcija takve mreže veza između različitih informacijskih sustava koja bi omogućavala dobivanje i uspoređivanje svih osobnih podataka sadržanih u tim sustavima. Tako dobiven skup podataka, svojevrstan "nadzorni profil", najviše zastrašuje običnog građanina[14]. Činjenica da postoji mogućnost da netko na jednom mjestu raspolaže podacima o, primjerice, zdravstvenom stanju, potrošačkim navikama, školskim ocjenama, knjigama posuđenima u knjižnici, broju posjeta zubaru, članstvu u udrugama, osobama kontaktiranim telefonom i elektronskom poštom, kažnjavanosti i prosječnim primanjima ne predstavlja tek opasnost na razini akademskih rasprava, već stvara pretpostavke za mnogovrsne oblike zloraba (od diskriminiranja/povlašćivanja na temelju netransparentnih i nerelevantnih kriterija do manipuliranja biračkim tijelom).

3. Posebno o pojedinim pitanjima

3.1. Tajnost podataka

I pravnici i sociolozi i psiholozi nedvojbeno bi se složili da je tajnost jednostavno neizbježna. Ponekad je nužna, ponekad korisna, ponekad opasna, a vrlo često i uzaludna. *Tko ima oči vidi, a tko uši čuje. Iz toga proizlazi uvjerenje da ni jedan smrtnik ne zna čuvati tajnu. Čija su usta nijema, taj će progovoriti vrhovima prstiju* (Freud). Tajna slovi za *jedno od najvećih dostignuća čovječanstva, budući da otvara mogućnost ulaska u drugi svijet uz onaj stvarni*

[13] *Vjesnik* od 09.11.2000, 20. str.

[14] Brezak, Milan. *Pravo na osobnost, Pravna zaštita osobnih podataka od zlouporabe* (Zagreb: Nakladni zavod Matice hrvatske, 1998). 29.

(Simmel).[15] Već zbog brojnih aspekata fenomena tajnosti pravo može učinkovito intervenirati u ovo područje samo djelomično. To, međutim, ne umanjuje važnost dovoljno dobrog reguliranja toga (malog) dijela.

Osnovnu shemu hrvatskih propisa o zaštiti tajnosti već smo iznijeli pod 2.1. Mislimo da aktualni hrvatski propisi s područja tajnosti podataka imaju sljedeće glavne nedostatke:

1. definiranje tajne isključivo formalnim elementima[16];
2. nedovoljno precizirani kriteriji klasifikacije i deklasifikacije;
3. preširok krug osoba ovlaštenih za (de)klasificiranje podataka;
4. prepuštanje znatnog dijela materije podzakonskom reguliranju;
5. potpuno izostavljanje testa pretežnosti interesa, koji bi bio primjeren u pojedinim situacijama;
6. nepostojanje nadzornog tijela s javnim ovlastima (ZZTP određuje osnivanje Vijeća za provjeru tajnosti, kao savjetodavnog tijela koje izdaje neobvezujuće obavijesti - tijela koje u vrijeme pisanja ovog rada /skoro četiri godine nakon stupanja ZZTP-a na snagu/ još uvijek nije utemeljeno).

3.2. *Osobni podaci*

Kao što smo već naveli, između triju pitanja kojima je posvećen ovaj rad zaštita osobnih podataka u hrvatskom je pravu još uvijek najnepotpunije regulirana.

Prema stajalištu Europske komisije za ljudska prava (*Van Oosterwijk protiv Belgije*, Izvj. Komisije iz 1979), *pravo na poštovanje "privatnog života" jest pravo*

[15] Cit. u: Halter, Hans, Misterija pokreće svijet, *Der Spiegel*, prenijeto u *Novom listu* od 13.09.1999.

Zanimljivo je usporediti dvije klasifikacije načina saznavanja tajni - jednu na teorijskoj (Scheppele), a drugu na novinarskoj razini (Halter). Prema Sheppeleu, tajna se odaje otkrivanjem, izdajom ili otjecanjem. Halter, pak, navodi ogovaranje, trač, laž i izdaju. U oba slučaja laž se povezuje s tajnom (cilj laganja često je upravo čuvanje tajne). Kod Scheppelea laž je kompliciraniji oblik tajne (tajna s pričom na vrhu). Halter ističe da laž ublažava šok pri otkrivanju tajne, ubrzava tijek dana te potpomaže usponu u društvu - Scheppele, Kim L., Legal Secrets: Equality and Efficiency in the Common Law (Chicago: Universitiy of Chicago Press, 1988), 11 i d.

[16] *Tajna je podatak koji je zakonom, drugim propisima, općim aktom ili drugim aktom nadležnog tijela donesenim na temelju zakona, određen tajnim* (čl. 2. st. 1. ZZTP). Sadržajni sastojak definicije tajne djelomice je propisan odredbama ZZTP-a (i na njemu utemeljenih podzakonskih propisa) o pojedinim vrstama i stupnjevima tajnosti (npr. čl. 6. - državna tajna te primjerično navođenje državnih i vojnih tajni u čl. 7. i 8). Kod službenih tajni, međutim, sadržaj tajnih podataka nije određen niti primjerično (čl. 12). Ako se poštuje uvjet određenosti propisom, praktički bilo koji podatak može se proglasiti tajnim.

privatnosti, pravo da se živi onako kako tko želi, zaštićen od javnosti... ono sadrži dakle, do određenog stupnja, pravo da se ustanove i razviju odnosi s drugim ljudskim bićima osobito na polju osjećajnosti, za razvoj i ispunjenje nečije vlastite osobnosti. Pritom, zahtjev da se poštuje privatan život automatski je ograničen na onaj opseg u kojem pojedinac svoj privatni život izlaže dodiru s javnim životom ili bliskoj vezi s ostalim zaštićenim interesima (*Brueggeman protiv SR Njemačke*, Izvj. Komisije iz 1977).[17]

Usporedbe radi, američki Vrhovni sud prihvaća pravo vlade da ograniči prikupljanje i širenje informacija o pojedinoj osobi, priznajući pritom četiri oblika takve privatnosti: *(1)* pravo da ne bude prikazan u "lažnom svjetlu" objavljivanjem lažnih činjenica; *(2)* pravo da ne dopusti da mu se ime i slika "koriste" za komercijalne vrijednosti; *(3)* pravo na publicitet osobi čije ime ima komercijalnu vrijednost; *(4)* pravo izbjegavanja objavljivanja "intimnih detalja".[18]

Jedan od najvažnijih, a rjeđe spominjanih aspekata privatnosti tiče se odnosa unutar pojedine organizacije (najčešće se radi o pitanju zaštite privatnosti na radnom mjestu). Newstrom i Davis navode tipične poslovne aktivnosti koje mogu utjecati na privatnost, među inim: detektore laži; testove osobnosti; medicinske preglede; nadzor nad životnim stilovima zaposlenika; nadzorne uređaje; kompjutorske banke podataka; istraživanje osobnih veza[19].

Na općenitoj razini, pravnom zaštitom osobnih podataka štiti se i pravo na osobnost. Pritom se javlja pojam informacijske osobnosti, koju Westin

[17] Gomien, Donna. *Kratak vodič kroz Europsku konvenciju o ljudskim pravima* (Zagreb: Organizator: Strasbourg: Vijeće Europe, 1996), 70-71.

Također, granice dopuštene kritike znatno su šire kad su u pitanju političari (javne osobe) nego kad se radi o privatnim osobama, jer se političari *dragovoljno i svjesno izlažu pomnom ispitivanju svake svoje riječi i djela, pa sukladno tome moraju iskazivati i veći stupanj tolerancije - Castells protiv Španjolske*, 1992, prema: Skupina autora, *Zakon o javnom priopćavanju* (Zagreb: VIV - inženjering, 2000), 167.

Polazeći od zajamčenog prava javnosti da bude informirana o svim javnim događajima, pojavama, osobama, predmetima i djelatnostima od javnog interesa, nesporno je i pravo javnosti da prima informacije o javnome životu javnih osoba. Nerijetko je, međutim, i privatni život javnih osoba važan za pravilno sagledavanje njihove javne djelatnosti i javnoga života. Pritom postoje tri osnovne skupine javnih osoba: *(1)* javni dužnosnici; *(2)* glumci, sportaši, gospodarstvenici i druge osobe poznate u društvenoj zajednici i uključene u pojedina društvena zbivanja (spomenute dvije skupine smatraju se tzv. *apsolutno javnim osobama*); *(3)* tzv. *relativno javne osobe* (javnosti inače nepoznate, ali zbog svog aktivnog sudjelovanja u određenim društvenim kontroverzijama, raspravama ili događajima postaju od interesa za javnost. Skupina autora, *Zakon o javnom priopćavanju*, 34-36.

[18] Skupina autora, *Priručnik o slobodi javne riječi*, 204-205.

[19] Newstrom, John W. - Davis, Keith, *Organizational Behavior, Human Behavior at Work*, 10th ed., Boston...: McGraw-Hill, 1997, 284-285.

definira kao *zahtjev pojedinaca, grupa ili institucija da samostalno odluče kada će, kako i koje informacije o sebi ustupiti drugima*. Informacijska osobnost podrazumijeva da pojedinac o tome odlučuje vodeći računa o svojim pravima i potrebama, ali i o pravima i potrebama zajednice u kojoj živi [20]

Prethodno spomenuti radni tekst Nacrta ZZOP-a ima nekoliko glavnih karakteristika:

1. širina predmeta zakona - cilj je obuhvatiti sve bitne aspekte zaštite osobnih podataka, kako u pogledu njihova sadržaja, tako i subjekata i načina obrade podataka, čime se jamči dovoljna razina cjelovitosti zaštite[21];
2. autoritativno i učinkovito nadzorno tijelo - predviđeno je utemeljenje državnog vijeća za zaštitu osobnih podataka, kao neovisnoga i profesionalnog tijela s javnim ovlastima (takvo je tijelo potrebno radi djelotvorne zaštite prava osoba, ali i radi ujednačavanja pravne prakse i razine pravne zaštite na ovom području)[22];
3. uravnotežena zaštita legitimnih interesa - primarni cilj zakona jest zaštita osobnih podataka (kao ustavnog prava), dok se pojedinim odredbama osigurava zaštita javnog interesa i interesa drugih osoba, osigurava ravnoteža s drugim ustavnim pravima (npr. pravom novinara na pristup informaciji) te legitimnim interesima javnosti (npr. ograničenjem zaštite osobnih podataka javnih osoba koji su u vezi s njihovim javnim položajem);
4. ograničavanje kaznenih odredbi samo na one povrede zakona koje ne predstavljaju kazneno djelo prema Kaznenom zakonu[23].

[20] Brezak. *Pravo na osobnost*. 22.

[21] Predviđena je zaštita svih podataka koji se odnose na određenu ili odredivu fizičku ili pravnu osobu, bez obzira na to kako su ti podaci izraženi, na koji se način obrađuju te tko ih prikuplja, obrađuje ili se njima koristi (iznimka su zbirke podataka koje vode fizičke osobe u kućanstvima za kućnu ili osobnu primjenu).

[22] Predviđene su tri temeljne skupine ovlasti državnog vijeća: *(1)* odlučivanje u postupku zaštite prava osoba i korisnika (sudska zaštita protiv odluka Državnog vijeća osigurava se u upravnom sporu); *(2)* nadzor nad djelovanjem sustava obrade osobnih podataka; *(3)* savjetodavna djelatnost.

[23] Pritom je od najveće važnosti odnos između odredbi budućeg ZZOP-a i čl. 133. st. 1. Kaznenog zakona (kazneno djelo nedozvoljene uporabe osobnih podataka): *Tko bez privole građana protivno uvjetima određenima u zakonu, prikuplja, obrađuje ili koristi njihove osobne podatke ili te podatke koristi suprotno zakonom dozvoljenoj svrsi njihova prikupljanja*... Pojmovi prikupljanja, obrade i korištenja osobnih podataka definirani su u temeljnim odredbama ZZOP-a. I *uvjeti određeni u zakonu* odnose se na uvjete koji će biti propisani ZZOP-om. *Zakonom dozvoljena svrha* može, osim u ZZOP-u, biti propisana i drugim zakonima.

Osim čl. 133. KZ, za zaštitu osobnih podataka relevantna su i kaznena djela u vezi s tajnošću podataka (kada su osobni podaci ujedno klasificirani), kazneno djelo povrede slobode izražavanja misli (čl. 107. st. 2), a neizravnije i

Usporedna zakonodavstva sadrže različite varijante reguliranja zaštite osobnih podataka, primjerice:

- zakonom o zaštiti osobnih podataka ili zaštita u okviru propisa o privatnosti;
- zaštita podataka samo fizičkih, odnosno i fizičkih i pravnih osoba;
- isključivanje ili uključivanje ručno vođenih zbirki osobnih podataka u sustav zaštite[24];
- nadzor putem posebnoga neovisnog tijela ili putem redovitih sudbenih i upravnih tijela.[25]

Često isticanje naročite osjetljivosti informatičke obrade osobnih podataka nije slučajno. *U prošlosti, špijuniranje naših osobnih navika bilo je teže jednostavno zato što su informacije bile razasute na različitim mjestima. Sada računala pohranjuju ogromne količine informacija o nama na jednome mjestu, memoriji računala, kojoj je putem telefonskih linija lako pristupiti bilo odakle*[26]. Mogućnost pohranjivanja, spajanja, manipuliranja i pristupa osobnim podacima, koju imaju računala, pruža razlog sumnji o mogućoj zlorabi, jer neovlaštena uporaba funkcija kompjutora može nezvanome omogućiti stvaranje potpunoga informacijskog profila pojedine osobe[27].

Smjernice OECD-a o zaštiti privatnosti i prekograničnom tijeku osobnih podataka (1980) te Konvencija Vijeća Europe o zaštiti pojedinaca u pogledu

kaznena djela povrede tajnosti glasovanja (čl. 119), povrede tajnosti pisama i drugih pošiljaka (čl. 130) te neovlaštenog snimanja i prisluškivanja (čl. 131).

[24] Dio zakonodavstava reguliranje zaštite osobnih podataka ograničava na informatičke sustave. Zbog njihovih kapaciteta i mogućnosti povezivanja nedvojbeno je da takvi sustavi predstavljaju najveći rizik zlorabe osobnih podataka. Osim države, kao "tradicionalnog zlorabitelja", u novije doba sve veća opasnost prijeti od privatnog sektora - legalnoga (primjerice, jake tvrtke, trgovački lanci, banke, osiguravajuća društva i sl.) ili ilegalnog (organizirani kriminal).

Kao što smo već naveli, prema radnom tekstu Nacrta prijedloga ZZOP-a zaštita ipak nije ograničena na informatičke sustave zbog, prema našem mišljenju, dvaju glavnih razloga: načelnoga (zaštitu ne treba ograničavati prema "tehničkom" kriteriju) i praktičnog (niža razina informatizacije u Hrvatskoj u usporedbi s većinom zemalja čija su zakonodavstva analizirana).

[25] Zakonsko uređenje zaštite osobnih podataka daleko je opsežnije u Europi negoli u Sjedinjenim Državama. Većina europskih zakona pokriva javni i privatni sektor. Automatska obrada osobnih podataka predmet je svih zakona, dok ručnu obradu uređuju, primjerice, njemački, norveški i francuski zakon. Istodobno, u Sjedinjenim Državama glavni su napori usmjereni na formuliranje legalnih prava pojedinaca radi ostvarivanja sudske zaštite - Brezak, *Pravo na osobnost*, 87-88.

[26] Dominick, Joseph R., The Dynamics of Mass Communication, 4th ed. (New York,...: McGraw-Hill, 1993), 582

[27] Brezak, *Pravo na osobnost*, 26.

automatske obrade osobnih podataka (1981) postavljaju sljedeće zahtjeve: *(a)* postojanje temeljnog zakona o zaštiti osobnih podataka, koji obuhvaća sve sustave u javnome i privatnom sektoru; *(b)* uređenje postupaka prikupljanja, obrade i korištenja osobnih podataka; *(c)* reguliranje odnosa između osobe, voditelja zbirke podataka i drugih korisnika; *(d)* osiguranje sudske zaštite; *(e)* utemeljenje specijalizirane nadzorne ustanove; (f) osiguranje utjecaja na sadržaj vlastitih osobnih podataka; *(g)* utvrđivanje obveze registracije i javnog objavljivanja svih zbirki osobnih podataka, napose kompjutoriziranih.

U radnom tekstu predložena je sljedeća struktura ZZOP-a:

I - Temeljne odredbe;

II - Načela zaštite osobnih podataka (zakonitost; svrhovitost; javna obavijest; točnost; sigurnost; zabrana prikupljanja, obrade i korištenja osjetljivih podataka[28]; zabrana korištenja nezakonito prikupljenih podataka; nezavisni nadzor);

III - Prikupljanje, obrada i korištenje osobnih podataka;

IV - Posebne kategorije osoba i podataka (osjetljivi podaci; podaci o javnim osobama; novinarski pristup osobnim podacima);

V - Iznošenje osobnih podataka iz Republike Hrvatske;

VI - Zbirke osobnih podataka i registri zbirki osobnih podataka;

VII - Prava osoba i zaštita prava osoba (materijalnopravne i procesnopravne odredbe te odredbe o ograničavanju prava osoba, tj. dopuštenim iznimkama od pojedinih načela zaštite osobnih podataka);

VIII - Nadzor nad djelovanjem sustava obrade osobnih podataka;

IX - Kaznene odredbe (prekršaji);

X - Prijelazne i zaključne odredbe.

Radni tekst Nacrta ZZOP-a sadrži moguća rješenja za dio situacija u vezi s temom ovog rada (osobni podaci javnih osoba te dostupnost osobnih podataka novinarima) putem testa pretežnosti interesa[29].

[28] Osjetljivi podaci, prema radnom tekstu, obuhvaćaju podatke o rasnom podrijetlu, političkim stajalištima, vjerskim i drugim uvjerenjima, sindikalnoj pripadnosti, zdravlju, seksualnom životu te podaci o kaznenim presudama i prekršajima.

[29] Radni tekst predvida da se osobni podaci javnih osoba smiju dati na korištenje, osim u zakonom opće predvidenim slučajevima, drugim korisnicima i kada za to postoje drugi važni razlozi, *ako interes korisnika ili opće*

3.3. *Pravo novinara na pristup informaciji*

Glavna je zadaća novinara prikupljanje i objavljivanje točnih i relevantnih podataka. Njihovo pravo na pristup informaciji, kao i ostale pravom priznate novinarske funkcionalne povlastice (npr. povjerljivost novinarskih izvora, posebne odredbe o isključenju odgovornosti za štetu, mogućnost isključenja protupravnosti kaznenih djela protiv časti i ugleda, pravo nesankcioniranog odbijanja naloga koji se protivi pravilima novinarskog zanimanja i etike), prvenstveno slijede iz posebne uloge koju mediji imaju u demokratskom društvu[30].

Usporedni pravni sustavi mogu se u pogledu prava novinara na pristup informaciji podijeliti u dvije glavne skupine:

- sustavi s predmnjevom dostupnosti podataka (najčešće uz negativnu enumeraciju iznimaka);
- sustavi bez navedene predmnjeve[31].

Hrvatsko pravo predstavlja "varijaciju" prve inačice: predmnjeva dostupnosti postoji, ali vrijedi samo za novinare[32]. Ostali subjekti nisu time unaprijed isključeni od pristupa informacijama, ali im pravo na pristup ovisi o posebnim propisima koji uređuju pojedina područja.

Novinari nemaju pravo pristupa informaciji u posjedu tijela javne vlasti koja je klasificirana kao državna ili vojna tajna (čl. 5. st. 3. ZJP). Osim ograničenja

javnosti da budu upoznati s tim podacima preteže nad interesom zaštite osobnih podataka osoba, a radi se o podacima koji su u vezi s javnim položajem osobe.

Predložena je i sljedeća "novinarska odredba": *Osobni podaci dostupni su novinarima u skladu s propisima o pravu novinara na pristup informaciji, osim kada interes za zaštitu osobnih podataka osobe preteže nad interesom ostvarivanja prava novinara na pristup informaciji.* Bit te odredbe je uravnotežena zaštita dvaju ustavnih prava: prava na zaštitu osobnih podataka i prava novinara na pristup informaciji. Novinari imaju pravo pristupa svim podacima u posjedu tijela javne vlasti koji nisu državna ili vojna tajna. Bez "novinarske odredbe" u ZZOP-u novinari bi, dakle, imali pravo pristupa i svim osobnim podacima koji ujedno nisu državna ili vojna tajna, što ogromna većina osobnih podataka nije.

[30] Europski sud za ljudska prava u slučaju *Lingens protiv Austrije* istaknuo je dvostruku ulogu medija, kao "opskrbljivača informacijama" i "javnog psa čuvara".

[31] U prvu skupinu, primjerice, pripadaju: Austrija, Nizozemska, Švedska (pravo na pristup informacijama jest ustavno pravo); Sjedinjene Države, Njemačka, Španjolska (predmnjeva prava na pristup, uz zakonodavnu razradu); Norveška, Francuska (posebni zakoni koji osiguravaju to pravo).

Tipičan primjer druge koncepcije je Ujedinjeno Kraljevstvo, s tradicionalnim naglaskom na zaštiti državne tajnosti.

Skupina autora, *Priručnik o slobodi javne riječi* (London: Article 19; Zagreb: Press data, 1998), 150.

[32] Opširnije o prijeporima koji se javljaju u vezi s takvom koncepcijom u: Rajko, Alen, Zaštita prava na pristup informaciji putem ustavne tužbe, *Hrvatska javna uprava*, god. 1. (1999), br. 3.

u pristupu informacijama, ZJP djelovanje novinara ograničava propisujući pravo na zaštitu privatnosti, dostojanstva, ugleda i časti, uz određene iznimke kod javnih osoba i osoba koje same privlače pozornost javnosti (čl. 6. i čl. 13. st. 2), kao i obvezu objavljivanja točnih, cjelovitih i pravodobnih informacija te zabranu objavljivanja nezakonito prikupljenih informacija i državnih i vojnih tajni (čl. 13. st. 1. i 3).

4. Moguća mjerila rješavanja sukoba

Kao polazište za ovaj dio analize nužno je uzeti različitost pravnog značaja razmatranih triju pitanja: pravo novinara na pristup informaciji i pravo na zaštitu osobnih podataka prava su ustavnog ranga, a zaštita tajnosti podataka nije. Ustavotvorčevo upućivanje na uređenje zaštite tajnosti podataka putem zakona nema karakter prava. Osim toga, smatramo da odredbu čl. 37. st. 2. Ustava treba shvatiti i kao instrument zaštite interesa javnosti, s obzirom na to da obvezno reguliranje pitanja tajnosti zakonom ograničava rizike imanentne podzakonskom reguliranju osjetljivih pravnih područja.

Osim ustavnih jamstava, prethodno navedeni međunarodni ugovori, što određuju pravo na poštovanje privatnoga i obiteljskog života te pravo na slobodu mišljenja i izražavanja, a koji su dio hrvatskoga pravnog poretka, također daju "nadzakonski" karakter pravu na zaštitu osobnih podataka i pravu novinara na pristup informaciji.

Spomenuta različitost pravnog značaja upućuje na nekoliko zaključaka.

1. U "trokutu" pitanja razmatranih ovim radom u svakome konkretnom slučaju pri ocjeni odnosa između zaštite osobnih podataka i prava na pristup informaciji treba poći od njihove načelno jednake pravne snage[33].
2. U situacijama u kojima se tajnost podataka nalazi u odnosu s druga dva pitanja, tajnost se javlja kao:
   - iznimka od predmnjeve dostupnosti informacija novinarima,

[33] Primjerice, Alaburić i Havkić (sa stajališta medijskog prava) navode da je u situacijama sukoba prava na slobodu izražavanja te prava na poštovanje i zaštitu privatnosti u demokratskim državama temeljni kriterij utvrđivanja granice slobode izražavanja opravdani interes javnosti. *Interes javnosti za primanje informacija o nečijoj privatnosti može se smatrati opravdanim samo ako je informacija u svezi s nekim javnim događajem, javnom djelatnošću ili javnim životom osobe.* Skupina autora, *Zakon o javnom priopćavanju*, 33.

- okolnost koja može dodatno zaštititi podatke koji su zaštićeni i propisima o zaštiti osobnih podataka, dok izostanak tajnosti sam po sebi osobne podatke ne čini dostupnima.

3. U situacijama u kojima je potrebno ocjenjivati odnos između svih triju pitanja (npr. novinar traži pristup informaciji koja je povjerljiva prema propisima o zaštiti tajnosti te istodobno nedostupna prema propisima o zaštiti osobnih podataka), informacija je dostupna ako su ispunjena dva kumulativna uvjeta:
   - riječ je o informaciji čija povjerljivost ne predstavlja iznimku od predmnjeve dostupnosti informacija novinarima (prema sadašnjim propisima, ako nije državna niti vojna tajna);
   - važnost javne dostupnosti informacije - osobnog podatka (što se ostvaruje posredovanjem novinara) preteže nad važnošću zaštite toga osobnog podatka za ostvarivanje prava na osobnost subjekta podatka.
4. Pojedina pravna područja već sadrže odredbe koje (izravno ili pomoću pravila tumačenja) predstavljaju mjerila pri ocjenjivanju odnosa između sukobljenih pitanja.

Pritom za test pretežnosti između prava novinara na pristup informaciji i prava na zaštitu osobnih podataka u dvojbenim slučajevima predlažemo sljedeća okvirna mjerila:

a) za pretežnost dostupnosti informacije novinaru nužno je da je riječ o informaciji koja je nedvojbeno javno relevantna, kako s motrišta demokratskih običaja i prevladavajućeg shvaćanja zajednice, tako i s motrišta pravila novinarske etike;

b) jednaki stupanj zaštite ne uživaju svi propisima zaštićeni osobni podaci: najjaču zaštitu trebaju uživati podaci neposredno vezani uz ostvarivanje prava na osobnost, naročito podaci koji nisu nastali zakonski nedopuštenim ponašanjem subjekta;

c) podaci koji su već dostupni javnosti u opsegu koji je (stvarno ili potencijalno) barem jednak opsegu dostupnosti do kojeg bi doveo njihov pristup novinaru upućuju na pretežniji interes prava na pristup informaciji;

d) zaštićenost osobnih podataka javnih osoba i osoba koje same privlače pozornost javnosti smanjuje se samo u pogledu podataka koji su u vezi s javnim položajem osobe ili događajima koji su već poznati javnosti;

e) zaštićenost osobnih podataka javnih osoba i osoba koje same privlače pozornost javnosti smanjuje se razmjerno stupnju poznavanja te osobe u javnosti, njenome formalnom položaju, stvarnoj moći i mjeri u kojoj ima koristi od svoga javnog položaja;

f) ako je osobni podatak dodatno zakonito zaštićen prema propisima o tajnosti podataka, da bi bio dostupan novinarima, potrebno je da interes javnosti preteže i nad interesom zaštite osobnih podataka i nad interesom koji je zaštićen klasifikacijom podatka.

PERSONAL DATA, SECRET DATA AND THE ATTITUDE OF THE PRESS TOWARDS INFORMATION

Summary

The author of the text analyses legal situations caused by relations among three questions: secrecy of data, protection of personal data and the right of the press to access to information. First, principal legal elements of the analysis (within the framework of the constitutional provisions and international agreements and laws) at the level of basic information are presented. Main characteristics of a real situation are described by typical cases of "information draught" and manipulation of personal data. Principal guidelines of the working version of the Draft Proposal of the Protection of Personal Data Act, relevant at the time of writing the text, are mentioned. In conclusion, measures for the solution of the conflict of legally protected interests connected with the three above-mentioned questions are proposed. In this connection, different legal significance of the questions under consideration is taken into account: the right of the press to access to information and the right to protection of personal data are constitutional rights, while the protection of secrecy of data is not. General criteria for the test of prevalence between the mentioned constitutional rights are suggested as well.

Key words: personal data, secret data, attitude towards information