KONCEPT REGULATIVNOG OKVIRA INFORMACIJSKE SIGURNOSTI

mr.sc. Aleksandar Klaić, dipl.ing.; dr.sc. Anita Perešin

SAŽETAK:

U radu se uvode i definiraju pojmovi politike informacijske sigurnosti i suvremenog informacijskog prostora. Širenje i kompleksnost informacijskog prostora, u odnosu na ranija razdoblja, zahtijeva i razvoj novog koncepta regulativnog okvira informacijske sigurnosti. U kontekstu navedenih definicija, u radu se raščlanjuje regulativni okvir informacijske sigurnosti prema vrsti akata kao što su zakoni, uredbe, pravilnici, norme ili etički kodeksi te se utvrđuje razlika između pojedinih vrsta propisa. Utvrđuje se i definira skup specifičnih vrsta podataka koje su dominantne s obzirom na zahtjeve informacijske sigurnosti te se daje prikaz regulative informacijske sigurnosti s obzirom na ove specifične vrste podataka. U radu se nadalje analiziraju tehnološki i društveni procesi koji su doveli do današnjih regulativnih standarda u području informacijske sigurnosti te se upućuje na važnost razumijevanja regulative, kako s aspekta upravljanja zahtjevima regulativne usklađenosti, koje predstavlja bitnu komponentu suvremenog poslovanja, tako i s aspekta razvoja informacijske sigurnosti, jer su regulativni okvir, njegova strategija i planiranje, danas glavni pokretači informacijske sigurnosti, neovisno o sektoru primjene.

Uvod

Sigurnosni standardi NATO-a i Europske unije, čije se uvođenje zahtijeva od svih država članica, obuhvaćaju, između ostalog, i zahtjeve za uređenjem područja informacijske sigurnosti te definiranjem nacionalne sigurnosne politike u tom području.

Prilikom uređivanja područja informacijske sigurnosti, potrebno je voditi računa o činjenici da se suvremena politika informacijske sigurnosti danas razvija u potpuno promijenjenom okruženju, u kojem je nekadašnji tradicionalni pristup informacijskoj sigurnosti u državnoj upravi, nakon raspada blokovske podjele svijeta, tehnološke revolucije u području informacijske i komunikacijske tehnologije te sveopće globalizacije, postao nedostatan. Promjena tehnoloških mogućnosti povlači za sobom promjenu načina ponašanja korisnika, a ove promjene donose potpuno izmijenjen spektar ugroza i ranjivosti, uz sveprisutne asimetrične ugroze, kakva je i suvremeni terorizam. Postupna evolucija tradicionalne politike informacijske sigurnosti, čiji korijeni sežu u doba hladnoratovske podjele svijeta, donosi promjene koje su u praksi uglavnom nedostatne i prespore. Iako je pristup području informacijske sigurnosti donekle različit u državnoj upravi i u pravnim osobama koje djeluju na tržištu, može se reći da je zbog sve većih sličnosti u okruženju, u poslovnim zahtjevima, pa i u metodologiji pristupa, kroz najbolju praksu informacijske sigurnosti ili, primjerice, upravljanje rizikom, nužan sličan i sveobuhvatan pristup području informacijske sigurnosti.

Upravo takav pristup zahtijeva donošenje koncepta regulativnog okvira informacijske sigurnosti, kojemu je svrha nacionalno područje informacijske sigurnosti uskladiti sa sigurnosnim zahtjevima NATO-a i EU-a i harmonizirati ga sa nacionalnim regulativnim sustavima drugih država članica. Kvalitetan koncept regulativnog okvira informacijske sigurnosti pritom prvenstveno zahtijeva jasno određen informacijski prostor. **Stoga u ovom radu polazimo od teze da je, s obzirom na širenje i kompleksnost suvremenog informacijskog prostora, nužno prilagoditi koncept nacionalne politike informacijske**

sigurnosti, odnosno slijedom toga reorganizirati i propisati odgovarajući nacionalni regulativni okvir informacijske sigurnosti.

Usklađivanje dosadašnje nacionalne prakse u RH sa sigurnosnim smjernicama NATO-a i Europske unije, rezultiralo je donošenjem nacionalne regulative i postavljanjem temelja za implementaciju propisanih mjera i standarda informacijske sigurnosti u svim državnim tijelima, tijelima jedinica lokalne i područne (regionalne) samouprave, pravnim osobama s javnim ovlastima i drugim pravnim osobama koje u svom djelokrugu koriste klasificirane i neklasificirane podatke. Skup, u tom kontekstu donesenih posebnih zakona (*Zakon o tajnosti podataka, Zakon o informacijskoj sigurnosti* i *Zakon o sigurnosnim provjerama*), uveo je i definirao pojmove kao što su *informacijska sigurnost, mjere i standardi informacijske sigurnosti, područja informacijske sigurnosti* te *klasificirani i neklasificirani podaci.*

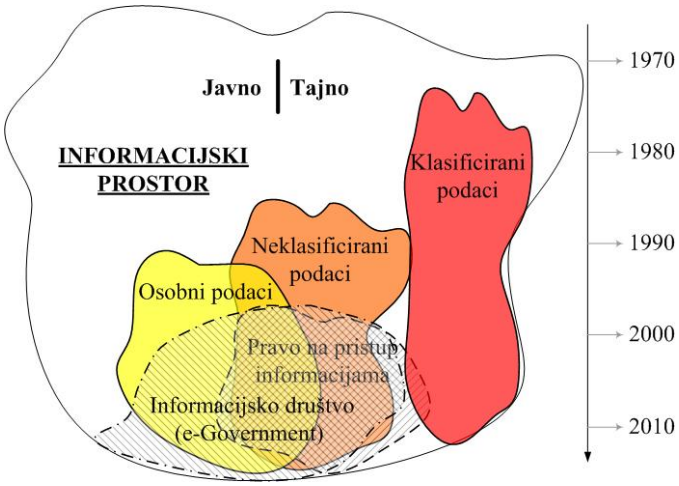
Informacijska sigurnost, u kontekstu navedenih posebnih zakona, promatra se primarno u okviru uvođenja propisanih mjera i standarda informacijske sigurnosti za zaštitu klasificiranih i neklasificiranih podataka. Takav pristup uobičajen je za uvođenje informacijske sigurnosti u rad državne uprave. Međutim, područje informacijske sigurnosti nužno je sagledavati šire od mehanizama nužnih za provedbu informacijske sigurnosti isključivo u području rada državne uprave, već zahtjeve informacijske sigurnosti, s obzirom na širinu informacijskog prostora, treba primijeniti i na suvremeno društvo u cjelini, koje postaje informacijsko društvo.

U radu se provodi analiza i definiranje **informacijskog prostora** u kojem se postupa s podacima, uvodi se i definira prikladni pojam **politike informacijske sigurnosti** te se definira **skup specifičnih vrsta podataka koje su dominantne s obzirom na zahtjeve informacijske sigurnosti** i ukazuje se na potrebu određivanja koncepta regulativnog okvira informacijske sigurnosti koji će moći zadovoljiti zahtjeve sigurnosti suvremenog informacijskog prostora.

1. Informacijski prostor

Informacijski prostor predstavlja virtualnu globalnu okolinu međusobno povezanih javnih i privatnih informacijskih sustava, u kojoj nastaju i prenose se različite vrste podataka, ali i specifični podaci koji su dominantni s obzirom na propise i zahtjeve informacijske sigurnosti. Slijedom toga potrebno je primijeniti mjere i standarde informacijske sigurnosti propisane za zaštitu povjerljivosti, dostupnosti i cjelovitosti podataka te dostupnosti i cjelovitosti informacijskih sustava u kojima se ti podaci obrađuju, pohranjuju ili prenose.

Suvremeni informacijski prostor stvara se tijekom posljednjih nekoliko desetljeća. U tom razdoblju čitav niz različitih trendova utjecao je na formiranje suvremene paradigme informacijskog društva i pripadajućeg informacijskog prostora. Analizom razdoblja od posljednjih nekoliko desetljeća mogu se utvrditi neke karakteristične faze kroz koje je oblikovanje javnog informacijskog prostora prolazilo, kao što je prikazano na *Slici 1.*



Slika 1. Stvaranje suvremenog informacijskog prostora [1]

1.1. Podjela informacijskog prostora

U razdoblju do sedamdesetih godina prošlog stoljeća, kako je prikazano na *Slici 1.*, informacijski prostor karakterizirala je izražena segmentacija informacijskog prostora u okviru pojedinih država, kao i oštra granica između javnog i tajnog informacijskog prostora. Ova oštra granica u to je vrijeme bila dodatno naglašena diskrecijskom mogućnošću odlučivanja državnih tijela o granicama između javnog i tajnog dijela informacijskog prostora. Tajni prostor pripadao je u potpunosti državnom sektoru u užem smislu, odnosno najvećim dijelom sigurnosno-obavještajnom, policijskom i vojnom dijelu tog sektora, a pravila klasificiranja podataka bila su gotovo potpuno zatvorena za širu javnost. Nužnost vojne, ali i obavještajno-sigurnosne suradnje između različitih država, sve više je profilirala postupke klasificiranja podataka te se na prijelazu sedamdesetih u osamdesete godine prošlog stoljeća sve jasnije utvrđuju koncepti, danas široko prihvaćene četvero-stupanjske klasifikacije tajnosti podataka, temeljene na stupnju štete od neovlaštenog otkrivanja klasificiranog podatka. Bitna komponenta ovog koncepta bila je jasna veza između stupnja tajnosti određenog klasificiranog podatka i skupa mjera i standarda informacijske sigurnosti kojima treba zaštititi podatak određenog stupnja tajnosti.

Sve jasniji zahtjevi sigurnosne politike u šezdesetim i sedamdesetim godinama prošlog stoljeća potiču stvaranje sigurnosnih modela za provedbu ciljeva sigurnosne politike, u prvom redu na informacijskim sustavima. Tako su nastali *rešetkasti model* (Lattice Model) i *Bell-La Padula model*, formalni sigurnosni modeli koji se bave kontrolom pristupa podacima na informacijskom sustavu, odnosno sigurnosnim kriterijem povjerljivosti tih podataka, ili primjerice *Biba model* koji je usmjeren na kriterij cjelovitosti podataka [3]. Sigurnosnim modelima, na formalni, matematički način, arhitektura informacijskog sustava prilagođava se ciljevima sigurnosne politike.

S obzirom da je sastavni dio informacijskog sustava u primjeni i njegovo okruženje, koje uz tehnički sustav obuhvaća i podatke na sustavu te korisnike sustava, nužan korak dalje bili su sigurnosni načini rada informacijskih sustava. Tako sigurnosni načini rada informacijskih

sustava: namjenski (engl. *dedicated*), na razini sustava (engl. *system high*), razdijeljeni (engl. *compartmented*) i multirazinski (engl. *multilevel*), povezuju stupanj tajnosti klasificiranih podataka na informacijskom sustavu, razinu sigurnosnih certifikata osoba koje pristupaju informacijskom sustavu, nužnost pristupa klasificiranom podatku u okviru djelokruga rada osobe (engl. *need-to-know*), kao i formalno odobrenje za pristup podacima na informacijskom sustavu.

Vidljivo je da uspostava sustava povjerenja prema osobama čini bitan i nužan element provedbe sigurnosne politike. Tako se, primjerice, u državnoj upravi, osobama koje pristupaju klasificiranim podacima, na temelju sigurnosne provjere izdaje sigurnosno uvjerenje (certifikat) odgovarajućeg stupnja tajnosti, usklađenog sa stupnjem tajnosti klasificiranih podataka kojima trebaju pristupati. Postupak sigurnosne provjere inicira državno tijelo, za svog zaposlenika koji u okviru djelokruga svog radnog mjesta ima potrebu pristupa (engl. *need-to-know*) određenim kategorijama klasificiranih podataka kao što su NATO ili EU klasificirani podaci, ili pojedinim nacionalnim kategorijama klasificiranih podataka, kao što su, primjerice, podaci o klasificiranim ugovorima u okviru nabave (princip razdvajanja nadležnosti). Izdavanjem sigurnosnog certifikata osobi te potpisivanjem izjave osobe o tome da je svjesna svojih prava i obveza u području tajnosti podataka, rukovoditelji pojedinih službi izdaju formalno odobrenje za pristup određenom fondu klasificiranih podataka ili odobravaju pristup na neformalnoj razini, razvođenjem pojedinog klasificiranog podatka osobi koja ima odgovarajući certifikat i poslovno zaduženje.

Ovakav koncept provedbe sigurnosne politike razvio se u državnim upravama tijekom sedamdesetih i osamdesetih godina prošlog stoljeća, isprva u najrazvijenijim državama svijeta, a kasnije i u ostalim demokratskim državama. Tako dolazi do stvaranja jasne i transparentne regulative vezane uz principe klasificiranja podataka, čime se tajni dio tadašnjeg informacijskog prostora transformirao u relativno transparentno, jasno ograničeno područje, odnosno u domenu klasificiranih podataka. S obzirom da su načela klasificiranja postala slična u različitim državama i pri tome javno propisana i transparentna, stvoreni su preduvjeti za učinkovitu međunarodnu razmjenu klasificiranih podataka i suradnju različitih država na problematici koja zahtijeva razmjenu klasificiranih podataka, kao što je vojna suradnja, ili borba protiv suvremenih ugroza, kao što je terorizam. Temelji međusobnog povjerenja država na taj su način sagrađeni na osnovi jasnih načela klasificiranja i zaštite podataka, odnosno na primjeni odgovarajuće, međusobno usklađene sigurnosne politike (npr. *Ugovor između Vlade Republike Hrvatske i Vlade Republike Bugarske o uzajamnoj zaštiti i razmjeni klasificiranih podataka*, NN MU 1/09).

Sigurnosna politika u osamdesetim godinama prošlog stoljeća i dalje je poticala jaku nacionalnu segmentaciju informacijskog prostora (zatvaranje podataka u nacionalne granice). Tek iznimno brz razvoj informacijske i komunikacijske tehnologije te brzo širenje interneta tijekom devedesetih godina, ublažava nacionalnu segmentaciju informacijskog prostora, povezujući nacionalne informacijske prostore različitih država u zajednički globalni informacijski prostor [4]. No, isto tako, u takvim okolnostima društvo postaje sve više svjesno potrebe zaštite od ugroza povezanih s rastućom i globalnom informacijskom tehnologijom. Bilo je to vrijeme, napose u Europskoj uniji [5], kada je započela sustavna regulacija općenitih koncepata privatnosti, kao i specifičnosti zaštite osobnih podataka, što je ubrzo postalo globalna paradigma razvijenog svijeta. Na taj je način domena osobnih

podataka postala posebno značajna u informacijskom prostoru jer su korisnici osobnih podataka i državna tijela i druge pravne osobe, a osobni podaci često se razmjenjuju u okviru međunarodne suradnje različitih država, ali i u okviru svakodnevnih poslova, kao što je, primjerice, sigurnost zračnog prometa.

Općeniti koncepti privatnosti pravnih osoba, odnosno zaštite intelektualnog vlasništva, tradicionalno korišteni u obliku poslovne tajne, tijekom devedesetih godina jasnije se definiraju i u državnom sektoru. Iako pod različitim nazivima i oznakama („*NATO Unclassified*“, „*EU Limitee“*, …), područje neklasificiranih podataka u državnom sektoru devedesetih godina postaje nezaobilazna domena podataka državne uprave. Slijedeći temeljne koncepte privatnosti, neklasificirane podatke karakterizira osjetljivost u smislu poslovnih ili službenih odnosa, pri čemu ti podaci nemaju svojstvo tajnosti te kao takvi ne mogu biti klasificirani stupnjem tajnosti. Ovakvi podaci, označeni oznakom „Neklasificirano“, predstavljaju mogućnost kojom se može, primjerice, spriječiti uvid javnosti u situacijama kada bi takav uvid otežavao daljnju provedbu aktivnosti na koje se odnosi sadržaj neklasificiranog podatka. Jedan od najboljih primjera za korištenje oznake „Neklasificirano“ jest planiranje i priprema budućih zakonskih akata u državnoj upravi, koji u fazi razrade mogu nositi oznaku „Neklasificirano“, kako bi se izbjeglo prerano javno komentiranje različitih opcija koje razmatra radna grupa koja radi na izradi prijedloga [6]. Takav način korištenja oznake „Neklasificirano“ ničim ne prejudicira kasniju proceduru, primjerice, kroz javnu raspravu ili prijedlog Vlade za upućivanje pravnog propisa na donošenje u parlament. U svim tim slučajevima oznake poput „Neklasificirano“ ili „Unclassified“, predstavljaju oznake za podatke koji nisu tajni, ali su namijenjeni samo za službeno postupanje određenih osoba (engl. *need-to-know*) i nije dopušteno njihovo objavljivanje. Na taj način uvedena je još jedna označena kategorija podataka, koja osigurava primjereno postupanje s podacima koji nisu tajni, ali nisu namijenjeni drugoj uporabi osim u službene svrhe. Uvođenje ove, neklasificirane domene podataka, iako donekle komplicira postupanje s podacima, u osnovi predstavlja poticaj državnoj upravi za smanjenje broja klasificiranih podataka i samim time za veću transparentnost rada državne uprave.

1.2. Povezanost segmenata informacijskog prostora

Procesi demokratizacije društva tijekom devedesetih godina dvadesetog stoljeća uvode u regulativnu praksu koncept poznat kao *pravo na pristup informacijama* (*Freedom of Information - FOI*). Krajem devedesetih, mnoge razvijene demokratske države, osobito članice EU-a, uvode ovaj koncept u svoju nacionalnu regulativu [6]. Cilj ovog koncepta bio je pomiriti međusobno kontradiktorne zahtjeve državne uprave za klasificiranjem (zatvaranjem) podataka te zahtjeve javnosti za transparentnošću (otvaranjem) rada državne uprave. U tom smislu važno je napomenuti da ovaj koncept nije u koliziji s podatkovnim domenama informacijskog prostora, kao što su klasificirana i neklasificirana domena, već upravo suprotno, ovim konceptom osigurava se dodatna kontrola podataka kojima se bavi državna uprava – kontrola javnosti. Načelo *prava na pristup informacijama* tako obuhvaća mogućnost uvida u neki dokument državne uprave ili dobivanja informacije o određenoj temi, ali pod propisanim uvjetima (pisani zahtjev, utemeljeni razlog i sl.). Pri tome, za neklasificirane podatke, državna tijela koja su vlasnici podataka moraju osigurati uvid u takve podatke prema propisanoj proceduri.

Što se tiče klasificiranih podataka, oni su izuzeti od direktne primjene ovog načela, ali se u većini država implementiraju dodatna načela nezavisne arbitraže između vlasnika podatka i tražitelja informacije, odnosno zakonske odredbe koje vlasnika klasificiranih podataka obvezuju na ocjenjivanje razmjernosti između interesa javnosti i zaštite vrijednosti koje su klasificiranjem određenog podatka zaštićene (nacionalna sigurnost). Najčešći organizacijski model koji se primjenjuje u različitim državama je model organizacije *državnog povjerenika za informacije*, koji provodi direktnu arbitražu između tražitelja podatka, koji potraživanje temelji na zakonu koji regulira načelo *prava na pristup informacijama* te vlasnika klasificiranog podatka, koji zaštitu (klasificiranje) podatka temelji na zakonu koji regulira tajnost podataka državne uprave. U RH je primijenjen nešto drugačiji model, u okviru kojeg je napravljena poveznica između *Zakona o pravu na pristup informacijama* (NN 172/03) i *Zakona o tajnosti podataka* (NN 79/07) te je u članku 16. *Zakona o tajnosti podataka* uvedena obveza da vlasnik klasificiranog podatka, koji je od interesa za javnost, provodi ocjenjivanje razmjernosti dva sukobljena interesa tajnosti i javnosti te da u okviru tog procesa zatraži mišljenje Ureda Vijeća za nacionalnu sigurnost, kao središnjeg državnog tijela za informacijsku sigurnost (engl. *National Security Authority - NSA*). *Zakon o tajnosti podataka* u članku 16. stavak 3., ostavlja otvorenim mogućnost naknadnog uvođenja državnog povjerenika za informacije nekim drugim zakonom, jer nije uobičajeno da takav povjerenik, kao procjenitelj zadužen za zaštitu transparentnosti ili javnosti rada državne uprave, bude reguliran *Zakonom o tajnosti podataka.*

Stvaranjem globalnog informacijskog prostora, uvelike temeljenog na rasprostranjenosti i sveprisutnosti interneta, javlja se potreba za učinkovitijim pristupom cjelokupnom informacijskom prostoru, u odnosu na pristup koji proizlazi iz korištenja i načela pojedinih podatkovnih domena informacijskog prostora, kao što je, primjerice, domena klasificiranih podataka. Pored nezaustavljive integracije nacionalnih informacijskih prostora u globalni informacijski prostor, međunarodne i nacionalne potrebe za komuniciranjem nameću promjenu i prilagodbu sigurnosnih politika i prakse komuniciranja s različitim vrstama podataka, kao što su osobni podaci ili klasificirani podaci. Takve promjene nije moguće postići bez opsežne i koordinirane prilagodbe kompleksne regulative u području tajnosti i privatnosti podataka. Upravo to se posljednjih desetak godina i događa te se, počevši od paradigme elektroničke državne uprave, preko šireg pojma informacijskog društva, prilagođavaju komponente nacionalnog zakonodavstva povezane s konceptima tajnosti i privatnosti [7]. Takve prilagodbe, zbog iznimnog tehnološkog iskoraka u području elektroničkih komunikacija i informacijske tehnologije te sveprisutnosti interneta, kao i posljedično stvorene nove društvene situacije – globalizacije, sežu u čitav niz zakona kojima se regulira područje rada davatelja elektroničkih komunikacijskih usluga, utvrđuju elektroničke inačice dokumenata i potpisa, postavljaju načela zaštite klasificiranih podataka, osobnih i drugih podataka, propisuju mjere i standardi zaštite podataka, odnosno potiče normizacija, kako u tehnološkom, tako i u sigurnosnom smislu.

Prilagodba nacionalnog sustava sigurnosnim zahtjevima NATO-a i EU-a, zahtijeva stvaranje koncepta regulativnog okvira informacijske sigurnosti koji će državnom, javnom i privatnom sektoru propisati, odnosno dati smjernice za zaštitu podataka u informacijskom prostoru.

2. Regulativni okvir informacijske sigurnosti

Opći koncept regulativnog okvira informacijske sigurnosti temelji se na kombinaciji zakonodavnih propisa, međunarodnih i nacionalnih normi te unutarnjih standarda svake pojedine organizacije (državnog tijela ili pravne osobe – tvrtke). U posljednjih desetak godina kompleksnost regulativnog okvira informacijske sigurnosti značajno raste. Razlozi tome leže u nizu faktora koji su donosili, donose ili će donositi promjene u današnjem suvremenom društvu, kao što su društveno-politički procesi poslije hladnog rata, globalizacija, velik tehnološki napredak krajem dvadesetog stoljeća, sveprisutnost interneta, velike krize poput terorističkog napada na SAD 11. rujna 2001. godine ili veliki gospodarski problemi poput propasti američke korporacije Enron iste godine, ali i zahtjevi demokratizacije poput koncepta *prava na informaciju* ili zaštite privatnosti. Svi ti procesi i događaji, u manjoj ili većoj mjeri, obilježavaju skup zakona koji čine regulativni okvir informacijske sigurnosti u različitim dijelovima svijeta, ali se ovakvi nacionalni regulativni okviri, zbog globalizacijskih procesa, sve češće primjenjuju i u drugim državama širom svijeta (npr. obveza primjene propisa određene države za inozemne tvrtke čije su dionice izlistane na određenoj dioničkoj burzi u toj državi).

Kako su procesi i događaji, poput spomenutih, imali različit utjecaj na društvo, tako je i konačan rezultat nacionalnih propisa informacijske sigurnosti u različitim dijelovima svijeta različit. No, unatoč tomu, mogu se prepoznati temeljni koncepti koji su zakonskom regulativom propisani te na različite načine primijenjeni u različitim državama, s obzirom na faktore kao što su legislativna tradicija, ustavna ograničenja, međunarodni integracijski procesi i slično. Iz toga proizlazi da je i kompleksnost međusobnih odnosa pojedinih odredbi različitih nacionalnih zakona i međunarodnih propisa sve veća. Sigurnost nije sama sebi svrha, već je stanje koje se želi postići u društvu, odnosno unutar nekog sektora društva, primjerice zdravstva, bankarskog sektora, gospodarstva, državnog sektora, građanstva itd. Kako su svi ti društveni sektori neminovno povezani, tako se i sigurnosni mehanizmi nužno dodiruju ili međusobno preklapaju u pojedinim slučajevima.

Sve ovo uvelike otežava utvrđivanje primjenjivosti pojedinih zakona i nekih specifičnih zakonskih odredbi, a pogotovo međusobnih interakcija više propisa. Utvrđivanje primjenjivosti pojedinih zakona može se pojednostaviti pomoću analize globalnog informacijskog prostora i interakcije informacijskog djelovanja određenog državnog tijela ili pravne osobe u okviru informacijskog prostora. Pri tome je potrebno promatrati faktore kao što su: međunarodni i nacionalni informacijski prostor i podaci, pristup i način korištenja interneta, odnosno objavljivanja podataka na internetu i u drugim javnim medijima, razina primijenjenog elektroničkog poslovanja s pratećim zahtjevima elektroničkog potpisa i dokumenta, korištenje određenih oblika tajnih podataka – klasificirani podaci, podaci označeni kao poslovna tajna, odnosno koncepta privatnosti podataka za pravne i fizičke osobe. Općenito rečeno, identifikacija primjenjive zakonske regulative može biti prilično težak zadatak, osobito u slučajevima kada određena organizacija, državno tijelo ili pravna osoba, surađuje ili posluje u međunarodnim okvirima, što u današnjem svijetu postaje nužnost i pravilo, a pri tome se kompleksnost regulativnog okvira informacijske sigurnosti samo povećava.

2.1. Sigurnosna politika u području informacijske sigurnosti

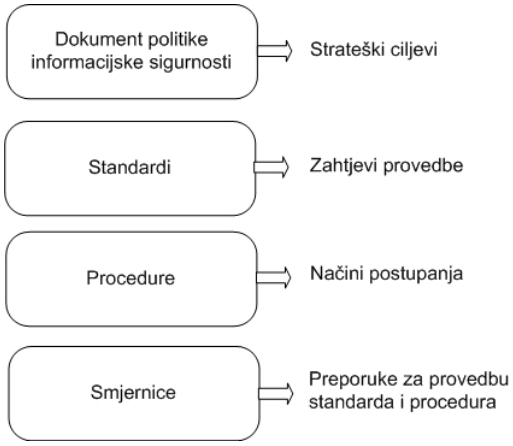
NATO i EU u svojim sigurnosnim direktivama, za sigurnosnu politiku u području informacijske sigurnosti koriste izraz *Security Policy* (hr. sigurnosna politika), a isti se termin u ovom užem značenju često koristi i u stručnoj literaturi iz područja informacijske sigurnosti. Međutim, važno je naglasiti da pojam sigurnosna politika ima i šire značenje koje je vezano uz pojam nacionalne sigurnosti. Suvremene sigurnosne politike u širem značenju Tatalović, Grizold i Cvrtila definiraju kao djelatnosti za pripremu osiguravanja od izvora budućih ugroza u prirodi, društvu i među društvima, dok u užem značenju one za njih predstavljaju zbroj svih mjera, djelatnosti i postupaka namijenjenih uspostavljanju i djelovanju sustava nacionalne sigurnosti [8].

S obzirom da je područje informacijske sigurnosti potrebno promatrati kao jednu od grana nacionalne sigurnosti, smatramo nužnim preciznije odrediti značenje pojma sigurnosne politike u području informacijske sigurnosti te stoga predlažemo uvođenje i definiranje pojma *politike informacijske sigurnosti.*

U tom smislu, **politika informacijske sigurnosti**, predstavlja dokumente kojima se utvrđuju mjere i standardi informacijske sigurnosti koje je potrebno primijeniti u informacijskom prostoru za zaštitu povjerljivosti, dostupnosti i cjelovitosti podataka te dostupnosti i cjelovitosti informacijskih sustava u kojima se ti podaci obrađuju, pohranjuju ili prenose.

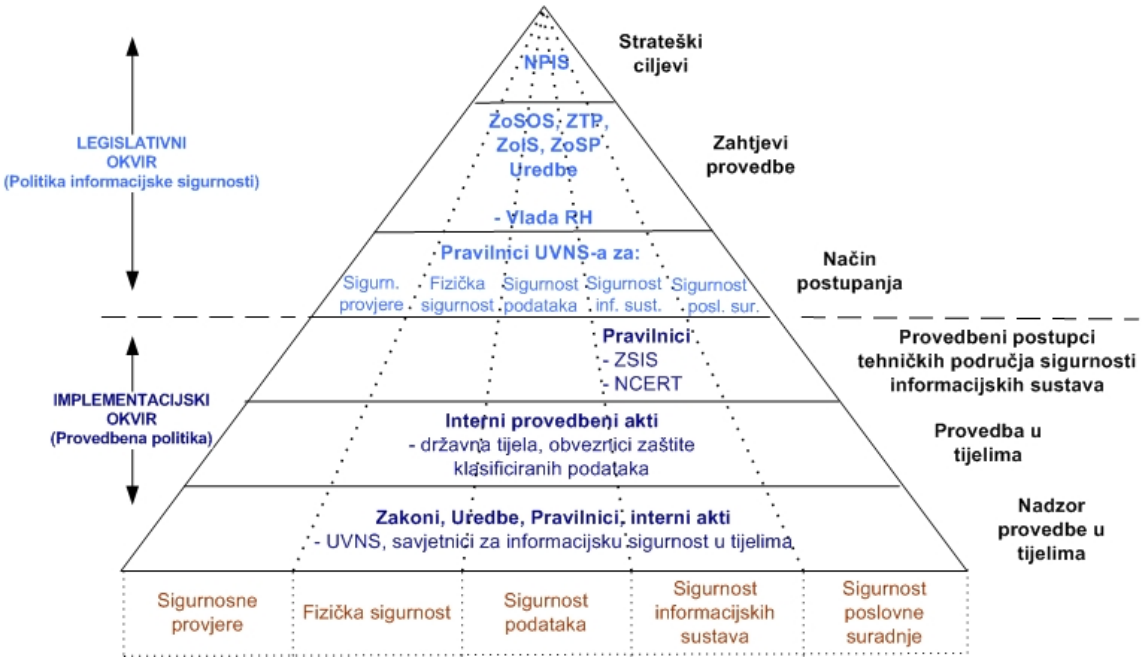
Politika informacijske sigurnosti koristi se i kao naziv za izjavu ili očitovanje najodgovornijih osoba (uprava tvrtke, čelnik državnog tijela, …) o uvjerenjima, ciljevima i razlozima te općenitim načinima kako doći do željenih postignuća u području informacijske sigurnosti, i to u obliku kratkog i konciznog dokumenta na općenitoj razini, bez specifičnosti i detaljnih opisa. Donošenje ovakvih dokumenata sigurnosne politike najčešće proizlazi iz zakonskih obveza, odnosno iz primjene normi kao što je HRN ISO/IEC 27001, a može biti i rezultat vlastite unutarnje inicijative određene institucije. Općenito, politika informacijske sigurnosti predstavlja hijerarhijski strukturiran skup dokumenata koji se, pored opisanog krovnog dokumenta, uobičajeno sastoji i od razine standarda, koji predstavljaju obvezujuće zahtjeve za provedbu sigurnosne politike, razine procedura, koje predstavljaju obvezujuće postupke te od razine smjernica ili naputaka, koje su preporučeni načini realizacije i stvaranja okvira za provedbu standarda i procedura (*Slika 2.*).

Kompleksnost općeg, krovnog dokumenta politike informacijske sigurnosti pritom ovisi o kompleksnosti organizacije i ciljeva koji se žele postići te su u tom smislu politike informacijske sigurnosti u državnom sektoru često vrlo kompleksne, jer u sebi sadrže i uspostavu mehanizama nužnih za organizaciju i upravljanje informacijskom sigurnošću u iznimno heterogenom okruženju kakvo je državna uprava [9]. Uz sve navedeno, politika informacijske sigurnosti se i funkcionalno raščlanjuje na više slojeva, pa obično razlikujemo opće politike na razini organizacije u cijelosti, funkcionalne politike po određenim područjima (npr. fizička sigurnost), kao i specifične politike te politike prihvatljivog korištenja (engl. *Acceptable Use Policy – AUP*) pojedinih resursa (npr. sustava, aplikacija i sl.) [10]. Bez obzira na razlike u formi dokumenata politike informacijske sigurnosti, pristupu i nazivlju, općenito rečeno, politikom informacijske sigurnosti uvijek se osigurava uvođenje minimalnih sigurnosnih zahtjeva u okviru određene organizacijske cjeline.



Slika 2. Hijerarhijske razine u skupu dokumenata politike informacijske sigurnosti

Na *Slici 3.* prikazan je primjer opisane hijerarhije propisa informacijske sigurnosti u državnom sektoru RH. Vrlo slični okviri regulative informacijske sigurnosti mogu se vidjeti i na primjerima drugih država, odnosno u međunarodnim organizacijama kao što su NATO ili EU.



Slika 3. Primjer hijerarhije propisa informacijske sigurnosti u državnom sektoru RH[1]

[1] NPIS = Nacionalni program informacijske sigurnosti
ZoSOS = Zakon o sigurnosno-obavještajnom sustavu RH (NN 79/06)
ZTP = Zakon o tajnosti podataka (NN 79/07)
ZoIS = Zakon o informacijskoj sigurnosti (NN 79/07)
ZoSP =Zakon o sigurnosnim provjerama (NN 85/08)

2.2. Hijerarhija propisa

Zakonodavni propisi obuhvaćaju široku paletu međunarodnih i nacionalnih zakonskih propisa. Zakonski i podzakonski akti međusobno se hijerarhijski nadograđuju, idući od općih prema posebnim propisima i od funkcionalnih prema provedbenim, odnosno od organizacijskih prema tehničkim propisima. Tako razlikujemo međunarodne ugovore (npr. *Zakon o potvrđivanju Ugovora između Republike Hrvatske i Europske Unije o sigurnosnim postupcima za razmjenu tajnih podataka*, NN MU 9/06) i zakone (npr. *Zakon o informacijskoj sigurnosti*, NN 79/07), čiju ratifikaciju, odnosno donošenje, redovito provode državni parlamenti, odnosno zakonodavni stup vlasti pojedine države.

Po hijerarhiji slijede uredbe (npr. *Uredba o mjerama informacijske sigurnosti*, NN 46/08) koje su u nadležnosti izvršne vlasti, odnosno vlade svake pojedine države te naposljetku pravilnici, odluke, naputci i smjernice različitih državnih tijela. Pri tome razina pravilnika, odluka, naputaka i smjernica može predstavljati podzakonsku razinu i primjenjivati se na nacionalnoj razini (npr. *Odluka o primjerenom upravljanju informacijskim sustavom,* HNB, NN 80/07, ili *Pravilnik o kriterijima za ustrojavanje radnih mjesta savjetnika za informacijsku sigurnost*, UVNS, NN 100/08), ali može predstavljati i interne akte samih državnih tijela za provedbu pojedinih, zakonom propisanih obveza unutar djelokruga tog državnog tijela (npr. *Pravilnik o tajnosti podataka obrane*, MORH, NN 39/08). Naputci i smjernice (npr. *Smjernice za upravljanje informacijskim sustavom u cilju smanjenja operativnog rizika*, HNB, ožujak 2006., www.hnb.hr/supervizija/), služe opisivanju preporučenih načina provedbe propisanih zahtjeva i postupanja, primjerice u području sigurnosti informacijskih sustava, a implementacija mjera definiranih ovakvim preporukama je poželjna, ali nije obvezujuća. U tom smislu, dokumenti s preporukama čine fleksibilne elemente regulativnog okvira informacijske sigurnosti, tako da se često koriste na onim mjestima gdje sigurnost nije moguće, nije potrebno ili nije poželjno strogo definirati.

Norme predstavljaju dokumente koji su odobreni od mjerodavnog nacionalnog ili međunarodnog tijela za normizaciju i koji za opću i višekratnu uporabu daju pravila, upute ili značajke za određenu vrstu aktivnosti ili njihove rezultate, s ciljem postizanja najboljeg stupnja uređenosti u danom okruženju (prikladnost namjene, optimizacija ograničenjem raznolikosti, spojivost različitih proizvoda, promicanje prednosti za društvo, kao što su sigurnost, zaštita zdravlja i okoliša, itd.) [11].

Kada govorimo o informacijskoj sigurnosti, norme predstavljaju rješenje zajedničkih potreba državne uprave i gospodarstva za jedinstvenim sustavima, primjerice u području upravljanja sigurnošću informacija (HRN ISO/IEC 27001) ili u području vrednovanja informacijske tehnologije (ISO/IEC 15408). Norme predstavljaju obvezujuće dokumente, ali isključivo u slučajevima kada na njih upućuju odredbe nekog zakonskog propisa, kao što je to, primjerice, u članku 38. *Uredbe o načinu pohranjivanja i posebnim mjerama tehničke zaštite posebnih kategorija osobnih podataka* (NN 139/04): *„Mjere, postupci i osobe ovlaštene za osiguranje, pohranjivanje i zaštitu sustava određuju se, ostvaruju i provjeravaju prema planu*

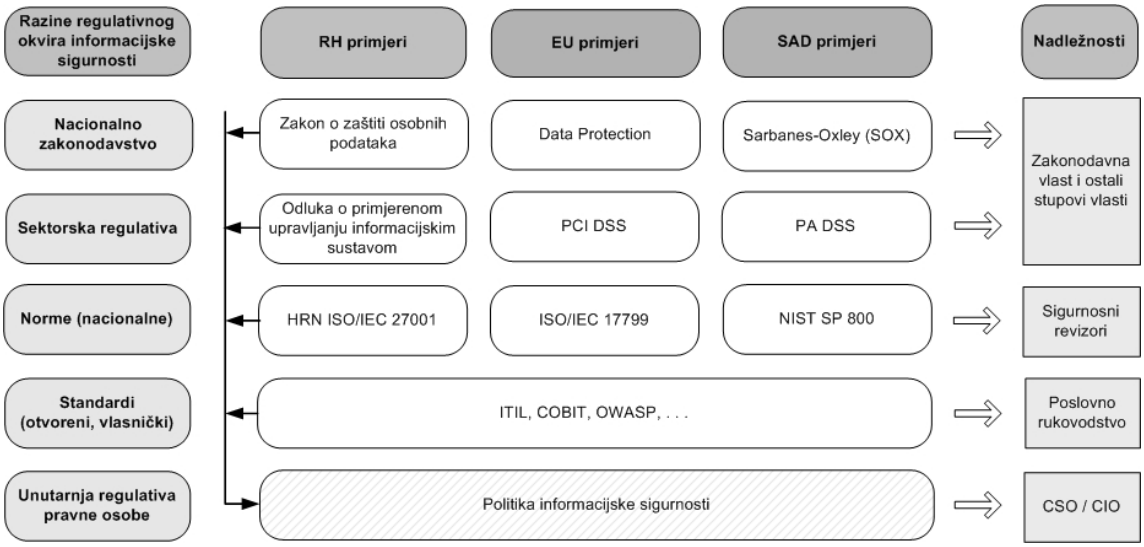
ZSIS = Zavod za sigurnost informacijskih sustava
NCERT = Nacionalni CERT

*kojeg donosi voditelj zbirke osobnih podataka, a u skladu s međunarodnim preporukama za to područje (*ISO 17799*).“*

Za razliku od normi, koje donose tijela za normizaciju, standardi predstavljaju dokumente pojedine institucije ili skupine institucija, namijenjene unutarnjoj uporabi u određenim institucijama (npr. *Standard za školske knjižnice*, NN 34/00) ili za potpuno otvorenu, javnu uporabu (npr. *IETF, RFC dokumenti*) [12], tzv. otvoreni standardi. Otvoreni standardi sve su više prisutni u području informacijske tehnologije. Razlog tomu je u iznimnoj dinamici razvoja, ali i u kompleksnosti područja informacijske tehnologije. Tradicionalni pristup normizaciji, kroz proces usklađivanja u tehničkim odborima nacionalnog normizacijskog tijela i kroz preuzimanje različitih međunarodnih normi u području informacijske tehnologije za nacionalnu uporabu (*ISO, IEC, CEN, ETSI i druge*), zbog dinamike razvoja tehnologije, pokazao se nedostatnim. Stoga se u području informacijske tehnologije najčešće koriste različiti otvoreni standardi, vlasnički standardi (engl. *proprietary*) ili de-facto standardi, tj. standardi koji su se nametnuli masovnim korištenjem (npr. Sony PlayStation ili Hayes AT skup naredbi za modeme). S obzirom da model vlasničkih (privatnih) standarda počiva na interesnoj grupaciji tvrtki koje usuglašavaju ili preuzimaju zajednički privatni standard (npr. tehnologije nasljednici DVD medija: Blue-ray disk i HD-DVD), takav pristup može dovesti do tržišne polarizacije, selektivnosti i netransparentnosti, odnosno do ograničenja tržišnog natjecanja te je stoga poželjna inicijativa državnog sektora usmjerena na poticanje otvorenih standarda i procesa normizacije [7].

Pored navedenog, potrebno je razlikovati i tzv. sektorsku ili industrijsku regulativu, ili regulativu vertikale poslovanja, kojom se na određeni način reguliraju, odnosno postavljaju zahtjevi koje moraju provesti sve pravne osobe koje se bave određenom vrstom djelatnosti, kao što je, primjerice, bankovni sektor ili sektor zaštitarske djelatnosti. Sektorsku regulativu mogu predstavljati neki od prethodno obrađenih slojeva u hijerarhiji propisa. Jedan od najreguliranijih sektora u smislu informacijske sigurnosti svakako je bankovni sektor. Može se reći da su vršni dokumenti sektorske regulative u bankovnom sektoru dokumenti Basel standarda, koji u stvari predstavlja međunarodni bankovni standard koji je kreirao Bazelski odbor za bankovni nadzor (*Basel Committee on Banking Supervision – BCBS*). BCBS se sastoji od predstavnika središnjih banaka i bankovnih regulatora iz nekoliko EU država, Japana i SAD-a, koji potiču međunarodnu kooperaciju banaka i izdaju smjernice za nadzor banaka. Iako aktualna inačica Basel II standarda nije zakon, njegovi zahtjevi preuzimaju se u zakonodavnoj praksi velikog broja država u svijetu (npr. EU direktive 2006/48/EC, 2006/49/EC, koje su obvezujuće za sve države članice EU) i propisuju se kroz različite nacionalne propise koji mogu biti zakoni, uredbe ili pravilnici, odnosno odluke središnjih banaka, kao nadležnih tijela. U RH je preuzimanje Basel II standarda utvrđeno donošenjem novog *Zakona o kreditnim institucijama* (NN 117/08) te čitavim nizom podzakonskih akata (npr. *Odluka HNB-a o upravljanju rizicima* i drugi akti: http://www.hnb.hr/propisi/hpropisi.htm).

Na S*lici 4.* prikazan je utjecaj različitih razina regulativnog okvira informacijske sigurnosti na politiku informacijske sigurnosti koja se provodi u pravnoj osobi, pri čemu su uzeti primjeri regulative, normi i standarda, tipični za RH, EU i SAD.



Slika 4. Utjecaj različitih razina regulativnog okvira informacijske sigurnosti na razvoj unutarnje politike informacijske sigurnosti pravne osobe[2]

2.3. Etički principi

Informacijska sigurnost u velikoj se mjeri temelji na zakonskim i drugim propisima koji osiguravaju uređeni okvir za uspostavu i upravljanje sustavom informacijske sigurnosti u određenom okruženju. No, zbog kompleksnosti ljudskog ponašanja i odnosa u društvu, propisi nisu uvijek odgovarajući način za rješavanje problematike postupanja osoba u nekim aspektima njihova rada. Tako sve aspekte sigurnosti, niti je moguće u potpunosti regulirati, niti bi ih se, u praktičnom smislu, moglo pravno procesuirati, posebice u slučajevima kada pojedini propisi daju mogućnost za različita tumačenja ili ostavljaju prostor nepotpuno uređenim u nekom od poslovnih segmenata (npr. uporaba privatnog softvera na poslovnim računalima, uporaba softvera koji ima licence za besplatno korištenje za fizičke osobe na računalima pravne osobe i sl.) [13]. U tom smislu, u određenim slučajevima koristi se etika, kao sustav vrijednosti i poželjnog ponašanja te se definiraju opći standardi prihvatljivog ponašanja, odnosno objektivno definirani standardi dobrog i lošeg ponašanja – etički kodeks.

U osnovi postoje dva načina etičkog pristupa: pristup temeljen na posljedici (teleologija) i pristup temeljen na pravilu (deontologija), pri čemu oba načina mogu biti promatrana u individualnom kontekstu (osoba - egoizam) ili univerzalnom kontekstu (društvo - utilitarizam) [13]. Etički kodeksi obično se utvrđuju za određeni profil zaposlenika ili određenu organizaciju (npr. *Etički kodeks državnih službenika*, NN 49/06, ili *ISC² Code of*

[2] PCI DSS – Payment Card Industry Data Security Standard
PA DSS – Payment Application Data Security Standard
NIST – U.S. National Institute of Standards and Technology
ITIL – Information Technology Infrastructure Library
COBIT – Control Objectives for Information Technology
OWASP – Open Web Applicatin Security Project
CSO/CIO – Chief Security/Information Officer

Ethics, https://www.isc2.org/cgi-bin/content.cgi?category=12) te predstavljaju kombinaciju etičkih pristupa prilagođenih kontekstu za koji su namijenjeni (npr. državni službenici u RH, odnosno svjetska strukovna udruga stručnjaka sigurnosti informacijskih sustava).

Regulativni okvir osigurava odgovarajuće kaznene i prekršajne mjere za kršenje odredbi propisanih zakonskim propisima, odnosno stegovne i disciplinske postupke za kršenje odredbi propisanih unutarnjim aktima pojedinih institucija. Osnovni princip etičkog kodeksa je postavljanje okvira za razmatranje etičnosti postupanja pojedinca koji je, ulaskom u strukovnu udrugu ili zaposlenjem, prihvatio obvezu poštivanja određenog etičkog kodeksa. Iako sličnog naziva, dva prethodno spomenuta etička kodeksa bitno se razlikuju. Etički kodeks državnih službenika samo proširuje okvire u kojima je moguće prepoznati i utvrditi kršenje drugih postojećih propisa koje državni službenici moraju poštivati. Etički kodeks ISC^2 organizacije uobičajen je za strukovne organizacije (profesionalna etika) i u sebi sadrži kompletnu proceduru procesuiranja etičkih sukoba, kroz uspostavu etičkih sudova, koncept prijavljivanja etičkih sukoba, procesuiranje pojedinačnih slučajeva kršenja etičkih principa te stegovno kažnjavanje članova strukovne organizacije kojima je utvrđeno kršenje odredbi etičkog kodeksa, sukladno pravilima strukovne organizacije.

3. Vrste podataka i regulativa informacijske sigurnosti

U nastavku rada provodi se analiza regulativnog okvira informacijske sigurnosti, kroz prethodno definirani informacijski prostor, identifikacijom primjenjivih zakona po domenama informacijskog prostora, koje su određene na temelju vrsta podataka. Kada govorimo o vrsti podataka, smatramo nužnim definirati **skup podataka koji su dominantni s obzirom na zahtjeve informacijske sigurnosti**, a taj skup čine: *klasificirani podaci*, *neklasificirani podaci*, *osobni podaci* i *podaci koji predstavljaju intelektualno vlasništvo u širem smislu*. Pritom se pažnja usmjerava na zakonom propisane zahtjeve u RH te na usporedbu stanja u RH s važnijim zahtjevima EU-a.

3.1. Klasificirani podaci

Klasificirani podatak predstavlja tajni podatak u vlasništvu državne uprave. To je podatak koji nadležno državno tijelo u propisanom postupku označi klasificiranim, jer je za njega utvrdilo zakonsku obvezu određivanja stupnja tajnosti. Klasificirani podatak je i svaki drugi podatak, kojeg nekoj državi tako označenog preda druga država, međunarodna organizacija ili institucija, sukladno odgovarajućem međunarodnom ugovoru o uzajamnoj zaštiti klasificiranih podataka.

Zakonom se obavezno propisuju kriteriji klasificiranja, način označavanja, postupanja i zaštite klasificiranog podatka. U RH je postupanje s klasificiranim podacima propisano sa tri posebna zakona: *Zakonom o tajnosti podataka* (NN 79/07), *Zakonom o informacijskoj sigurnosti* (NN 79/07), *Zakonom o sigurnosnim provjerama* (NN 85/08) te nizom pripadajućih podzakonskih akata – uredbi, pravilnika i naputaka. U Europskoj uniji zaštita klasificiranih podataka određena je sigurnosnom politikom Vijeća EU, a propisana Odlukom Vijeća EU o prihvaćanju sigurnosne regulative Vijeća broj 2001/264/EC od 19. ožujka 2001.

godine (kasnije je doneseno više nadopuna), odnosno usklađena je s Odlukom Europske komisije o amandmanima na interna pravila postupanja broj 2001/844/EC, ECSC, Euratom od 29. studenoga 2001. godine (kasnije je doneseno više nadopuna).

Vlasnik klasificiranog podatka uvijek je određeno državno tijelo ili pravna osoba s javnim ovlastima, jer se zakonom propisuje kontrolni mehanizam koji ovlast klasificiranja daje vrlo usko, za najviši stupanj tajnosti, najmanjem broju državnih tijela, a za niže stupnjeve tajnosti nešto većem broju državnih tijela. Korisnici klasificiranih podataka mogu u osnovi biti sva državna tijela i pravne osobe s javnim ovlastima, u najširem smislu, od središnje do lokalne vlasti, odnosno u sva tri stupa vlasti, izvršnom, zakonodavnom i sudbenom, kada im tijelo koje je vlasnik klasificiranog podatka takav podatak dostavi u okviru službenog postupanja.

Sukladno članku 13. stavku 4. *Zakona o tajnosti podataka* (NN, 79/07), nadležno državno tijelo odgovorno je za klasificiranje podataka i za znanstvene ustanove, zavode i druge pravne osobe, kada temeljem zakonskih obveza koje koordinira to državno tijelo, rade na projektima, pronalascima, tehnologijama i drugim poslovima od sigurnosnog interesa za Republiku Hrvatsku. U tim slučajevima ovo državno tijelo nadležno je i za usklađivanje posebnih zakonskih obveza tih pravnih osoba (npr. obveze iz područja obrambenih priprema, sukladno *Zakonu o obrani*, NN 33/02, 76/07) s općim propisima informacijske sigurnosti i postupanjem središnjeg državnog tijela za informacijsku sigurnost - Ureda Vijeća za nacionalnu sigurnost.

Korisnici klasificiranih podataka mogu biti i sve pravne osobe koje s državnim tijelima, vlasnicima klasificiranih podataka, sklope klasificirani ugovor u okviru kojeg razmjenjuju klasificirane podatke. Ovako definirani vlasnici klasificiranih podataka, korisnici klasificiranih podataka te ugovaratelji klasificiranih ugovora, čine obveznike *Zakona o informacijskoj sigurnosti* u smislu provedbe propisa o klasificiranim podacima.

Obveza uzajamne zaštite klasificiranih podataka danas predstavlja jedan od najvažnijih zahtjeva pri međunarodnoj državnoj suradnji (Interpol, Europol, međunarodne mirovne misije i sl.). Takve obveze utvrđuju se bilateralnim međunarodnim ugovorima između dvije države ili multilateralnim međunarodnim ugovorima s međunarodnim organizacijama (NATO, EU, …). Međunarodne ugovore za RH usklađuje, i u ime Vlade RH potpisuje, Ured Vijeća za nacionalnu sigurnost kao hrvatski NSA, što je praksa u državama članicama NATO-a i EU-a. Nakon potpisivanja ovakvog međunarodnog ugovora, Vlada takve ugovore upućuje na ratifikaciju u Hrvatski sabor, gdje oni, nakon ratifikacije, postaju obvezujući dio državne pravne regulative. Na taj način međunarodni ugovori, jednako kao i nacionalni zakoni, obvezuju sve subjekte u državi koji koriste određene međunarodne klasificirane podatke. Štoviše, ukoliko su zahtjevi informacijske sigurnosti u ratificiranom međunarodnom ugovoru oštriji od zahtjeva propisanih nacionalnim zakonodavstvom, na međunarodne klasificirane podatke razmijenjene u okviru tog ugovora primjenjuju se zahtjevi iz međunarodnog ugovora.

Međunarodnim ugovorima osiguravaju se minimalni zahtjevi informacijske sigurnosti obje ugovorne strane (bilateralni) ili svih članica međunarodne organizacije (multilateralni), koji se tijekom pregovaranja usklađuju sa specifičnostima nacionalnog zakonodavstva iz područja informacijske sigurnosti. Primjena odredbi međunarodnih ugovora o uzajamnoj

zaštiti klasificiranih podataka obveza je svih, prije definiranih vlasnika klasificiranih podataka, korisnika klasificiranih podataka te ugovaratelja klasificiranih ugovora, koji u svom radu koriste određene međunarodne klasificirane podatke (npr. slanje nacionalnog klasificiranog podatka izvan državnih granica, prijem i korištenje međunarodnog klasificiranog podatka, stranka ugovaratelj međunarodnog klasificiranog ugovora i sl.).

Pored međunarodnih ugovora, uobičajeno se koriste i međunarodni akti za provedbu ugovora. Takve međunarodne akte potpisuju nadležna državna tijela (npr. *Sigurnosni aranžman između Ureda Vijeća za nacionalnu sigurnost (UVNS) Republike Hrvatske, Ureda za sigurnost Glavnog tajništva Vijeća Europske Unije (GSCSO) i Uprave za sigurnost Europske Komisije (ECSD) za zaštitu klasificiranih podataka razmijenjenih između Republike Hrvatske i Europske Unije*, listopad 2007., www.uvns.hr). Ovisno o vrsti i značaju međunarodnog akta, postoje dva načina zaključivanja ugovora koje provodi nadležno državno tijelo, prethodnim slanjem Vladi na donošenje zaključka i odluke o potpisivanju, ili slanjem obavijesti o provedenom potpisivanju međunarodnog akta.

3.2. Neklasificirani podaci

Podatak bez utvrđenog stupnja tajnosti, kada se koristi u službene svrhe, može biti bez oznake ili označen oznakom „Neklasificirano“. Podatak koji je bez oznake, nema ograničenja uporabe i pristupa osoba. Podatak koji je označen oznakom „Neklasificirano“ koristi se samo u službene svrhe i može biti dostupan isključivo onim fizičkim osobama, državnim tijelima i pravnim osobama, koje imaju potrebu korištenja takvog podatka u službene svrhe i radi obavljanja poslova iz njihova djelokruga (Članak 7. *Uredbe o mjerama informacijske sigurnosti,* NN 46/08).

Svaki podatak koji je Republici Hrvatskoj predala druga država, međunarodna organizacija ili institucija s kojom Republika Hrvatska surađuje, a označen je oznakom „Neklasificirano“, odnosno istovrsnom inozemnom oznakom, u skladu s odgovarajućim međunarodnim ugovorom koji je Republika Hrvatska potpisala, koristi se samo u službene svrhe i može biti dostupan isključivo onim fizičkim osobama, tijelima i pravnim osobama, koje imaju potrebu korištenja takvog podatka u službene svrhe i radi obavljanja poslova iz njihova djelokruga.

Najčešće se pojam i uporaba neklasificiranih podataka reguliraju istim zakonom kojim i klasificirani podaci (u RH je to *Zakon o tajnosti podataka*, NN 79/07). Kako je već prije naglašeno, šira uporaba podataka označenih oznakom „Neklasificirano“ zamjetna je u svijetu tijekom posljednjih desetak godina. To je razdoblje u kojem dolazi do intenziviranja zahtjeva za transparentnost rada državne uprave te je u sklopu toga ova kategorija podataka vrlo bitna jer omogućava odgovarajuće postupanje s podatkom koji nije tajan, ali je na određeni način osjetljiv za uvid javnosti i treba se koristiti isključivo u službene svrhe. Neklasificirani podaci, jednako kao i klasificirani podaci, tipični su za državnu upravu te su obveznici primjene propisa o neklasificiranim podacima tijela središnje državne i lokalne vlasti, odnosno institucije sva tri stupa vlasti, izvršnog, zakonodavnog i sudbenog.

Zaštita neklasificiranih podataka u državnoj upravi gotovo se redovito provodi prema istim standardima koji su propisani i za zaštitu osobnih podataka. Razlog tome je prvenstveno značaj državne uprave u smislu zaštite osobnih podataka, jer je državna uprava, slikovito rečeno, „tvornica osobnih podataka“ te gotovo bez iznimke možemo reći da svako državno tijelo uspostavlja i vodi neku vrstu baze podataka koja u sebi sadrži osobne podatke građana. To je osobito naglašeno u sektoru upravnih poslova, sudbenom i sigurnosnom sektoru, sektoru zdravstva ili pak zemljišno-katastarskim poslovima. Primjenom istih standarda zaštite na neklasificirane podatke (podaci koji nisu tajni, ali se koriste samo u službene svrhe), kao i na osobne podatke, znatno se pojednostavljuje realizacija zaštite podataka, a same mjere i standardi koji se primjenjuju postaju učinkovitiji. U tom smislu i rješenje propisano u RH vodi se opisanom logikom te se u članku 8. *Uredbe o mjerama informacijske sigurnosti*, utvrđuje obveza primjene skupa mjera informacijske sigurnosti, sukladno normama za upravljanje informacijskom sigurnošću HRN ISO/IEC 27001 i HRN ISO/IEC 17799 [14].

3.3. Osobni podaci

Zakon o zaštiti osobnih podataka (NN 103/03, 118/06, 41/08) utvrđuje zaštitu osobnih podataka u RH, odnosno zaštitu privatnosti, koja je obvezujuća za sve pravne i fizičke osobe, bilo u državnom, bilo u privatnom sektoru, kada prikupljaju, obrađuju ili koriste osobne podatke o fizičkim osobama. Osobni podaci su, u smislu ovog Zakona, identifikacijski broj, ali i svi podaci koji se odnose na identificiranu osobu ili osobu koja se putem tih podataka može identificirati.

Bitno je naglasiti da bi odredbe ovog Zakona u najvećoj mjeri trebale biti provedene u državnom sektoru. Počevši od rođenja, definiranja matičnih podataka i određivanja identifikacijskih brojeva, preko školovanja, zaposlenja, kupnje nekretnina, automobila i sl., evidencije o fizičkim osobama vode se u nadležnim državnim tijelima, odnosno različitim pravnim osobama s javnim ovlastima. S druge strane, pravne osobe iz privatnog sektora također su obveznici ovog Zakona, primjerice banke, uslužne ili trgovačke tvrtke koje vode evidencije o svojim klijentima i sl. Tako je primjena mjera za zaštitu osobnih podataka nužna u širokom spektru pravnih osoba i državnih tijela. Upravo stoga se *Uredba o načinu pohranjivanja i posebnim mjerama tehničke zaštite posebnih kategorija osobnih podataka* (NN 139/04), u članku 38. oslanja na međunarodnu normu ISO 17799, jednako dostupnu i primjenjivu, kako za državni, tako i za privatni sektor.

Ukoliko se veliki broj osobnih podataka fizičkih osoba i pripadajuća zaštita privatnosti provode spomenutim konceptom zaštite putem primjene međunarodne norme, onda je logično rješenje koristiti isti koncept zaštite općenito za zaštitu privatnosti u državnoj upravi [7] [15]. Upravo ovakva logika je poveznica s označenim neklasificiranim podacima i člankom 8. *Uredbe o mjerama informacijske sigurnosti* (NN 46/08).

Koncept *Zakona o zaštiti osobnih podataka* prati odgovarajuće propise EU-a, prvenstveno Direktivu 95/46/EC EU Parlamenta i Vijeća od 24. listopada 1995. o zaštiti pojedinaca s obzirom na obradu i prijenos osobnih podataka [16], odnosno Konvenciju iz Strasbourga iz 1981. godine, (European Treaty Series - No. 108) i njene kasnije dopune i izmjene. Nadalje,

direktiva 2002/58/EC odnosi se na obradu osobnih podataka fizičkih osoba i zaštitu privatnosti u elektroničkim komunikacijama, što je u RH usklađeno *Zakonom o elektroničkim komunikacijama* (NN 73/08).

Države članice EU-a, kao i države koje su na putu u EU, u nekoj fazi integracijskih procesa imaju sličan koncept zaštite osobnih podataka, kojem se u EU pridaje veliki značaj. S druge strane, SAD ima potpuno drugačiji pristup području zaštite privatnosti te nemaju poseban zakon kojim bi se štitila privatnost na način kako to radi EU. U SAD-u se zaštita osobnih podataka propisuje „prema potrebi" pojedinim specijalnim zakonima koji osobne podatke obuhvaćaju regulirajući pojedine sektore u državi, u okviru kojih se koriste osobni podaci građana SAD-a. Tako, primjerice, HIPAA[3] regulira sigurnost i privatnost zdravstvenih podataka građana SAD-a, a GLB[4] regulira privatnost osobnih podataka klijenata pojedinih institucija unutar financijskog sustava SAD-a (banke, fondovi, osiguravajuće kompanije i sl.).

Upravo zbog različitog koncepta zaštite osobnih podataka, česti su problemi u području zaštite osobnih podataka na relaciji EU-SAD, počevši od načina poslovanja tvrtki na ovim tržištima (International Safe Harbour Principles, Odluka Europske Komisije 2000/520/EC), pa do razmjene podataka o putnicima koji putuju iz zemalja EU u SAD (Sporazum EU-SAD od 28. lipnja 2007. godine o obradi i slanju PNR-a[5] od zrakoplovnog prijevoznika koji leti za SAD, Ministarstvu domovinske sigurnosti SAD-a – DHS-u).

3.4. Intelektualno vlasništvo

Intelektualno vlasništvo predstavlja temelj razvoja suvremene ekonomije, odnosno društva znanja, na sličan način kako je privatno vlasništvo predstavljalo temelj razvoja tržišne ekonomije [17]. Pod pojmom intelektualnog vlasništva podrazumijevamo autorska prava (stvaratelji književnih, glazbenih, umjetničkih i znanstvenih djela) i autorskom pravu srodna prava (prava umjetnika izvođača, proizvođača fonograma, organizacija za radiodifuziju, filmskih producenata, nakladnika i proizvođača baza podataka). Intelektualno vlasništvo u širem smislu obuhvaća i pojam industrijskog vlasništva koji uključuje patente, žigove, oznake geografskog porijekla, industrijski dizajn (zaštita vanjskog izgleda, odnosno pojavnosti nekog proizvoda), kao i poslovnu tajnu. Čitav niz zakona uređuje ovo područje u RH: *Zakon o autorskom i srodnim pravima* (NN 167/03), *Zakon o patentima* (NN 78/99), *Zakon o žigu* (NN 173/03), *Zakon o industrijskom dizajnu* (NN 173/03), *Zakon o oznakama zemljopisnog podrijetla i oznakama izvornosti proizvoda i usluga* (NN 78/99) te *Zakon o zaštiti topografija poluvodičkih proizvoda* (NN 173/03).

Osnovne razlike u različitim pravnim institutima koji se koriste u okviru intelektualnog vlasništva nalaze se u različitim konceptima ostvarivanja prava, u dužini zakonske zaštite, kao i u obimu prava koji se pojedinim pravnim institutom štiti. Tako je, primjerice, osnovna razlika između autorskih prava i patenta u tome što se autorska prava stječu samim stvaranjem određenog djela ili rada, nisu prenosiva i traju 70 godina nakon smrti autora, dok se pravo patenta stječe u okviru propisanog postupka koji provodi nadležno tijelo te se

[3] Health Insurance Portability and Accountability Act, SAD, 1996.
[4] Gramm-Leach-Bliley Act, SAD, 1999.
[5] Passenger Name Record – PNR

može prenijeti na druge osobe ugovorom o licenci, a traje između 10 i 20 godina, ovisno o vrsti provedenog postupka patentiranja. Nacionalna prava intelektualnog vlasništva prilično su usklađena u svijetu, što uglavnom nije slučaj s drugim granama prava, a ovdje je ta usklađenost posljedica vrlo ranih (počevši od 19. stoljeća) multilateralnih ugovora, poput *Pariške konvencije o zaštiti industrijskog vlasništva* iz 1883. godine. U *Tablici 1.* prikazana je usporedba načina zaštite intelektualnog vlasništva kroz koncept autorskog prava, patenta i poslovne tajne, s obzirom na čimbenike kao što su pravna zaštita koju pružaju, trajanje zaštite i sl.

Tablica 1. Usporedba autorskog prava, patenta i poslovne tajne u RH

	Autorsko pravo	**Patent**	**Poslovna tajna**
Objekt zaštite	Izražavanje ideje, ne sama ideja	Izum: način kako nešto radi	Tajna, neka prednost u tržišnom natjecanju
Javna objava zaštićenog objekta	Da, intencija je promovirati objavljivanje	Projekt registriran u Državnom zavodu za intelektualno vlasništvo	Ne
Zahtjev distribucije objekta	Da	Ne	Ne
Način registracije	Vrlo jednostavno, autor samostalno ili automatizmom	Vrlo komplicirano, zastupnici na području industrijskog vlasništva	Nema registracije
Trajanje	70 godina nakon smrti autora	10 do 20 godina od registriranja	Neograničeno
Pravna zaštita	Tužba kada se neautorizirane kopije prodaju	Tužba ako se izum kopira	Tužba ako je poslovna tajna neovlašteno otkrivena

Iako je koncept intelektualnog vlasništva originalno zamišljen kao zaštita za objekte poput knjiga, pjesama ili fotografija, ovaj koncept danas se u određenoj mjeri primjenjuje i na digitalne objekte i programska rješenja (softver). Autorsko pravo uobičajeno se primjenjuje na podatkovne medije s instalacijskim kopijama softvera koji se dostavljaju korisnicima. Na taj način može se uspješno zaštititi objektni kod softvera koji se distribuira, ali ne i izvorni kod, jer se zaštitom autorskih prava ne štiti ideja (u ovom slučaju algoritam), već samo način izražavanja ideje (u ovom slučaju instalacijska distribucija softvera). Patenti, kao sredstvo zaštite softvera, nisu primjenjivi, jer se u smislu patenta softver tretira kao apstraktna ideja - algoritam te nije patentibilan, osim u slučaju kada može biti dio procesa koji se patentira, ali kao samostalni softverski dio niti tada nije zaštićen. Poslovna tajna je najprimjenjivija za softver, jer omogućava zaštitu izvornog koda, uz istovremenu distribuciju objektnog koda zaštićenog autorskim pravom. No, poslovna tajna ne pruža zaštitu od reverznog inženjeringa, što u određenim slučajevima treba uzeti u obzir. Hardver, kao što su čipovi ili diskovne jedinice, u osnovi mogu biti patentirani, a za ugrađeni softver (engl. *firmware*) bolje je rješenje zaštite poslovna tajna. Programska dokumentacija zaštićena je autorskim pravima, jednako kao i sadržaj weba, koji predstavlja medij zapisa, poput knjige ili fotografije. Imena internetskih domena, tvrtki i proizvoda, kao i komercijalni simboli, štite se kao robni znakovi (žigovi).

Digital Millennium Copyright Act, donesen 1998. godine u SAD-u, pokušao je koncepte intelektualnog vlasništva prilagoditi digitalnim objektima (npr. uvođenje prava pričuvne kopije kupljenog digitalnog medija sa zvučnim ili video sadržajem). No, problem kopiranja u digitalnom svijetu nemoguće je riješiti principima nastalim u analognom svijetu, zbog

suštinske razlike između digitalnog i analognog svijeta, koja proizlazi iz činjenice da je digitalna kopija, za razliku od analognih kopija objekata poput knjiga, fotografija i pjesama, istovjetna digitalnom originalu. Upravo stoga, suvremena zakonska rješenja idu za tim da kupnju digitalnih objekata tretiraju više kao pravo najma, odnosno korištenja, a manje u smislu tradicionalnog poimanja kupnje (SAD, *No Electronic Theft Act*, 1997.). Na taj način učinkovitije se sprječava daljnja distribucija digitalnih objekata, čak i kada nije predmet zarade (npr. servisi kao MP3.com, Napster ili općenito „*peer-to-peer*" servisi).

Poslovna tajna predstavlja jedan od načina zaštite intelektualnog vlasništva. U većini pravnih sustava poslovna tajna tumači se kao informacija koja nije poznata stručnoj javnosti, koja na određeni način donosi ekonomsku korist svom vlasniku te čiju tajnost vlasnik poslovne tajne u razumnim okvirima nastoji sačuvati. U tom smislu poslovna tajna može biti određena poslovna praksa, odnosno način postupanja, određeno znanje do kojeg se u poslovnom sustavu došlo ili bilo koja druga informacija koja poslovnom subjektu pomaže u natjecanju s konkurencijom. Pravni sustav mora osigurati okvire korištenja poslovne tajne (tajni podaci pravnih osoba – tržišnih subjekata) na sličan način kako je to uređeno za područje klasificiranih podataka (tajni podaci državne uprave – državnih tijela). Uvjeti korištenja poslovne tajne utvrđeni su *Zakonom o zaštiti tajnosti podataka* (NN 108/96) te je i nakon stupanja na snagu novog *Zakona o tajnosti podataka* (NN 79/07), poglavlje VIII. Poslovna tajna, iz *Zakona o zaštiti tajnosti podataka* iz 1996. godine, ostalo na snazi. Nadalje, *Kaznenim zakonom* (NN 110/97, 27/98, 50/00, 129/00, 51/01, 111/03, 190/03, 105/04, 84/05, 71/06, 110/07, 152/08) utvrđuju se kazne za kršenje odredbi o poslovnoj tajni koje moraju biti donesene na odgovarajući način. To znači da podatak mora biti utvrđen kao poslovna tajna zakonom, drugim propisom ili općim aktom trgovačkog društva, ustanove ili druge pravne osobe, ako predstavlja proizvodnu tajnu, rezultate istraživačkog ili konstrukcijskog rada, odnosno drugi podatak zbog čijeg bi priopćavanja neovlaštenoj osobi mogle nastupiti štetne posljedice za gospodarske interese vlasnika podatka (trgovačko društvo, ustanovu ili drugu pravnu osobu).

Jedan od široko primjenjivanih načina korištenja poslovne tajne je u okviru procesa javne nabave koju provodi državna uprava u zemljama EU-a, ali i u RH, jer je donošenjem *Zakona o javnoj nabavi* (NN 110/07), ovo područje u velikoj mjeri usklađeno sa zahtjevima EU-a. Stoga je, između ostalog, na snazi i odredba po kojoj svaki ponuđač, prilikom dostavljanja svoje ponude u okviru predmeta javne nabave, može dijelove te ponude označiti kao poslovnu tajnu, ukoliko ne želi da ostali ponuđači budu upoznati s određenim dijelovima njegove ponude.

U okviru propisivanja poslovne tajne, pravne osobe uobičajeno koriste različite oznake za klasifikaciju stupnja tajnosti pojedinih podataka, kao što su npr. „Povjerljivo", „Osjetljivo" i sl. Iako načini klasifikacije, odnosno označavanja tajnosti podataka u pravnim osobama, mogu biti različiti, zajedničko im je da moraju biti propisani internim aktima pravne osobe te moraju obuhvatiti koncept upoznavanja zaposlenika s obvezama i odgovornostima za zaštitu ovakvih, posebno označenih podataka.

Zaključak

U radu se uvode i definiraju pojmovi suvremene politike informacijske sigurnosti i informacijskog prostora, analizira se utjecaj razvoja informacijskog prostora na suvremenu politiku informacijske sigurnosti te se definira i utvrđuje skup specifičnih podataka koji su dominantni s obzirom na zahtjeve suvremene politike informacijske sigurnosti. Razumijevanje ovih pojmova važno je za razumijevanje i donošenje koncepta regulativnog okvira informacijske sigurnosti i njegovu što kvalitetniju implementaciju na nacionalnoj razini.

Definiranje i određivanje okvira suvremenog informacijskog prostora u kojem se prenose različite vrste podataka, važno je za utvrđivanje vrsta podataka za čiju je zaštitu potrebno primijeniti određene mjere i standarde informacijske sigurnosti kako bi se, s jedne strane osigurala zaštita njihove povjerljivosti, dostupnosti i cjelovitosti, ali i istodobno poštivali koncepti prava na pristup informacijama i zaštite privatnosti.

Uvođenjem pojma *politika informacijske sigurnosti* odredili smo uži termin u području sigurnosne politike koji će jasnije ukazivati na područje na koje se odnosi, što je naglašeno i njegovom definicijom prema kojoj politika informacijske sigurnosti predstavlja dokumente kojima se propisuju mjere i standardi informacijske sigurnosti koje je potrebno primijeniti u informacijskom prostoru za zaštitu povjerljivosti, dostupnosti i cjelovitosti podataka te dostupnosti i cjelovitosti informacijskih sustava u kojima se ti podaci obrađuju, pohranjuju ili prenose. Politika informacijske sigurnosti predstavlja hijerarhijski strukturiran skup dokumenata koji se sastoji od krovnog dokumenta, razine standarda, koji predstavljaju obvezujuće zahtjeve za provedbu sigurnosne politike, razine procedura, koje predstavljaju obvezujuće postupke te od razine smjernica ili naputaka, koje su preporučeni načini realizacije i stvaranja okvira za provedbu standarda i procedura. U radu je opisana hijerarhija propisa informacijske sigurnosti u državnom sektoru RH, kao primjer okvira regulative informacijske sigurnosti kakav se može vidjeti i na primjerima drugih država, odnosno u međunarodnim organizacijama kao što su NATO ili EU. Međutim, važno je istaknuti da iako se informacijska sigurnost u velikoj mjeri temelji na zakonskim i drugim propisima koji osiguravaju uređeni okvir za uspostavu i upravljanje sustavom informacijske sigurnosti u određenom okruženju, zbog kompleksnosti ljudskog ponašanja i odnosa u društvu, u radu je naglašeno kako sve aspekte sigurnosti nije moguće u potpunosti regulirati te se ističe kako je u određenim slučajevima potrebno primijeniti etičke principe, kao sustav vrijednosti i poželjnog ponašanja prilikom zaštite podataka.

Definiranje skupa podataka koji su dominantni s obzirom na zahtjeve informacijske sigurnosti, koji čine klasificirani podaci, neklasificirani podaci, osobni podaci i podaci koji predstavljaju intelektualno vlasništvo u širem smislu smatrali smo nužnim radi određivanja osnovnih smjerova razvoja suvremene politike informacijske sigurnosti, osobito s aspekta regulativnog okvira.

Na taj način dokazana je početna teza da je**, s obzirom na širenje i kompleksnost suvremenog informacijskog prostora, nužno prilagoditi koncept nacionalne politike informacijske sigurnosti, odnosno slijedom toga reorganizirati i propisati odgovarajući nacionalni regulativni okvir informacijske sigurnosti.** Naime, regulativni okvir te njegova

strategija i planiranje, danas su pokretač većine najvažnijih procesa u području informacijske sigurnosti, neovisno o sektoru primjene te su samim time ključni za razumijevanje i daljnji razvoj informacijske sigurnosti.

Predmet daljnje analize ovog područja svakako treba biti sigurnost ovako definiranog informacijskog prostora, koja se treba temeljiti na analizi sigurnosnog okruženja, kao posljedice razvoja informacijskog prostora te na aspektima privatnosti i odgovornosti, kao i strategiji razvoja sigurnosne svijesti u najširim slojevima društva. Sigurnost informacijskog prostora treba predstavljati stratešku i preventivnu zadaću svake države koja slijedi suvremene koncepte razvoja informacijskog društva. U tom je smislu također potrebno izvršiti daljnju raščlambu regulativnog okvira te utvrditi zahtjeve koji se postavljaju politici informacijske sigurnosti u okviru suvremenog informacijskog prostora.

LITERATURA

[1] Klaić, A., Information Security Requirements in the Information Systems Planning Process, Conference Proceedings of the 17th International Conference Information and Intelligent Systems (IIS), Faculty of Organisation and Informatics, Varaždin, 2006, p. 265-269

[2] Klaić, A., Uloga industrijskog sektora u sustavu informacijske sigurnosti (nova legislativa u RH), pozvano predavanje, Microsoft Security Days 2006, Zagreb, Hrvatska, 2.-3.10.2006

[3] Anderson, R., Security Engineering, Wiley, 2001

[4] Commission communication COM(2005)229 final of 1 June 2005 to the Council (52005DC0229), the European Parliament, the European Economic and Social Committee and the Committee of the Regions on "i 2010 – a European Information Society for growth and employment", http://eur-lex.europa.eu/en/index.htm

[5] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995, on the protection of individuals with regard to the processing of personal data and on the free movement of such data, http://eur-lex.europa.eu/en/index.htm

[6] Council of Europe, Committee of Ministers, Recommendation Rec(2002)2 of the Committee of Ministers to Member States on Access to Official Documents (Adopted by the Committee of Ministers on 21 February 2002 at the 784th meeting of the Ministers' Deputies)

[7] Nacionalni program informacijske sigurnosti (NPIS), Središnji državni ured za eHrvatsku (SDUeH), http://e-hrvatska.hr/sdu/hr/Dokumenti/StrategijeIPrograma

[8] Tatalović, S., Grizold, A.; Cvrtila, V., Suvremene sigurnosne politike, Golden marketing - Tehnička knjiga, Zagreb, 2008., str. 10-11.

[9] Council Decision, Adopting the Council's Security Regulations, 19 March 2001, http://eur-ex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2001:101:0001:0066:EN:PDF , 2001/264/EC

[10] Peltier, T.R., Information Security Policies and Procedures, Auerbach Publications, 2004

[11] Hrvatski zavod za norme (HZN), http://www.hzn.hr/osnovnin.html

[12] Internet Engineering Task Force (IETF), http://www.ietf.org/

[13] Pfleeger, C.P., Pfleger, S.L., Security in Computing, Prentice Hall, 4th Ed., 2007
[14] HRN ISO/IEC 27001 i HRN ISO/IEC 17799, http://www.hzn.hr/
[15] BSI Standard 100-1 Information Security Management Systems (ISMS), BSI-Standard 100-2: IT-Grundschutz Methodology, BSI-Standard 100-3: Risk Analysis based on IT-Grundschutz, http://www.bsi.bund.de/english/publications/bsi_standards/index.htm
[16] Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data (95/46/EC)
[17] Katulić, T., Uvod u zaštitu intelektualnog vlasništva u Republici Hrvatskoj, Zagreb 2006., CARNet, http://e-knjiznica.carnet.hr/e-knjige/Intelektualno%20vlasnistvo/Intelektualno_vlasnistvo_u_RH.pdf