# Zaštita tajnosti podataka - regulatorni okvir i procedure u postupanju policijskih službenika

**Šutalo, Slaven**

**Master's thesis / Diplomski rad**

**2022**

*Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj:* **University of Split, University Department of Forensic Sciences / Sveučilište u Splitu, Sveučilišni odjel za forenzične znanosti**

*Permanent link / Trajna poveznica:* https://urn.nsk.hr/urn:nbn:hr:227:007416

**SVEUČILIŠTE U SPLITU**

**SVEUČILIŠNI ODIJEL ZA FORENZIČNE ZNANOSTI**

ISTRAŽIVANJE MJESTA DOGAĐAJA

DIPLOMSKI RAD

# ZAŠTITA TAJNOSTI PODATAKA – REGULATIVNI OKVIR I PROCEDURE U POSTUPANJU POLICIJSKIH SLUŽBENIKA

SLAVEN ŠUTALO

Split, rujan, 2022.

**SVEUČILIŠTE U SPLITU**

**SVEUČILIŠNI ODIJEL ZA FORENZIČNE ZNANOSTI**

ISTRAŽIVANJE MJESTA DOGAĐAJA

DIPLOMSKI RAD

# ZAŠTITA TAJNOSTI PODATAKA – REGULATIVNI OKVIR I PROCEDURE U POSTUPANJU POLICIJSKIH SLUŽBENIKA

MENTOR:izv.prof.dr.sc. MARIJA BOBAN

SLAVEN ŠUTALO

502/2019

Split, rujan, 2022.

**Rad je izrađen u**: Grude, Bosna i Hercegovina

**pod nadzorom**: izv.prof.dr.sc. Marije Boban

**u vremenskom razdoblju od** srpnja 2022. **do** rujna 2022. **godine**

**Datum predaje diplomskog rada: 09. rujna 2022. godine**

**Datum prihvaćanja rada: 19. rujna 2022. godine**

**Datum usmenog polaganja: 23. rujna 2022. godine**

**Povjerenstvo: 1. Prof. dr. sc Jozo Čizmić**

**2. doc. dr. sc. Marina Carić**

**3. izv. prof. dr. sc. Marija Boban**

# SADRŽAJ

# 1. UVOD

Danas živimo u svijetu tehnologije. Društvene mreže imaju monopol nad svim ostalim oblicima ljudske interakcije. Služe nam kao oblik kontakta s vanjskim svijetom i predstavljanja slike o sebi u javnosti. Nije problem podijeliti određene osobne podatke, no možda biste trebali pažljivije razmisliti o tome što se događa s informacijama koje uopće ne dijelimo.

Svi cijenimo svoju privatnost, ali nismo uvijek svjesni trenutaka kada je ona ugrožena. Nedavni skandal s najpoznatijom društvenom mrežom Facebook, mnoge je osvijestio o opasnostima koje vrebaju na internetu, pa su društvene mreže bile prisiljene promijeniti svoju politiku privatnosti podataka.

Međutim, ne može se pouzdano znati je li se nešto promijenilo. Politika privatnosti je nešto s čime se korisnici slažu prilikom korištenja bilo koje web stranice, a većina ljudi na to ne obraća pozornost. Također je moguće da korisnici nesvjesno pristanu na nešto što bi smatrali kršenjem vlastite privatnosti. [1]

Ključni pojmovi vezani uz temu zlouporabe podataka označavaju pojam osobnih podataka, odn. podatke koji se pripisuju određenoj osobi, te pojam privatnosti ili pravo svake osobe na vlastitu privatnost. Prema *Zakonu o zaštiti osobnih podataka*,[2] osobni podaci su definirani kao „svaka informacija koja se odnosi na identificiranu fizičku osobu ili fizičku osobu koju je moguće identificirati; osoba koja se može identificirati je osoba čiji se identitet može utvrditi izravno ili neizravno, posebice na temelju identifikacijskog broja ili jedne ili više karakteristika specifičnih za njezin fizički, psihički, mentalni, ekonomski, kulturni ili društveni identitet.”[3]

[1] M. Boban, *Sigurnost i zaštita osobnih podataka - pravni i kulturološki aspekti : doktorska disertacija*. Zagreb : Filozofski fakultet u Zagrebu : Odsjek za informacijske znanosti, 2012. Str. 11.;
[2] Zakon o zaštiti osobnih podataka Republike Hrvatske, dostupno na: https://www.zakon.hr/z/220/Zakon-o-zaštiti-osobnih-podataka (19.7.2022.);
[3] M. Boban, *Sigurnost i zaštita osobnih podataka - pravni i kulturološki aspekti : doktorska disertacija*. Zagreb : Filozofski fakultet u Zagrebu : Odsjek za informacijske znanosti, 2012. Str. 11.;

# 2. CILJ RADA

Cilj pisanja ovog diplomskog rada jest prikazati značaj zaštite tajnosti podataka, na temelju regulativnog okvira i procedure u postupanju policije. Prikazivanjem značenja sigurnosti i sigurnosti podataka, cilj je uvesti čitetelja u glavni dio, odnosno razradu same teme.

## 2.1. Hipoteze

Hipoteze ovog rada su:

- Zaštita tajnosti podataka se ogleda u pravilnom rukovođenju podatcima i dokumentima koji su u vlasništvu policijskih službenika za vrijeme trajanja određenog slučaja na kojem policija postupa prema svojim ovlastima.
- Zaštita podataka u policijskim postupanjima, u sklopu informacijske sigurnosti, ogleda se u tajnosti komunikacija između policijskih službenika s jedne i počinitelja kaznenih djela s druge strane.
- Informacijska sigurnost i zaštita osobnih podataka čine temelj policijske djelatnosti i uspjeha njihovog djelovanja na određenim slučajevima.
- Tajnost podataka doprinosi uspješnom i bržem okončanju istrage.
- Kvalitetan način postupanja s podatcima, kao i zaštita istih, pridonosi uspjehu obavljanja policijskih poslova i postupanja.

# 3. KODEKS POLICIJSKE ETIKE

U ovom se poglavlju prikazuje komentirani oblik policijskog etičkog kodeksa Bosne i Hercegovine.[4] Tekst je pisan na spomenutom kodeksu koji se temelji na Zakonu o policijskim službenicima Županije Sarajevo.[5] Policijskim etičkim kodeksom se uređuju standardi i pravila ponašanja policijskih službenika Uprave policije Ministarstva unutrašnjih poslova Kantona Sarajevo, način na koji pristupaju izvršavanju radnih i drugih zadataka i druga pitanja od značaja za navedenu oblast.[6]

## 3.1. Opće odredbe

Kodeks utvrđuje etičke i pravne smjernice za profesionalno obavljanje poslova policijskih službenika. Kodeks je usklađen i donesen po modelu Kodeksa policijske etike koji su usvojile sve policijske agencije u Bosni i Hercegovini. Kodeks je usklađen sa standardima Europskog kodeksa policijske etike koji je usvojilo Vijeće Europe.[7]

Ciljevi kodeksa su:

1 objasniti što se od policijskih službenika očekuje u određenim okolnostima i što se može dogoditi ako se ne pridržavaju propisanih pravila ponašanja,
2 određuju ponašanje policijskih službenika u određenim situacijama
3 unaprijediti zaštitu ljudskih prava i sloboda kroz kolektivnu i individualnu odgovornost u primjeni prava

[4] POLICIJSKI ETIČKI KODEKS ZA POLICIJSKE SLUŽBENIKE UPRAVE POLICIJE MINISTARSTVA UNUTRAŠNJIH POSLOVA KANTONA SARAJEVO, dostupno na: https://mup.ks.gov.ba/sites/mup.ks.gov.ba/files/policijski_eticki_kodeks.pdf (20.7.2022.);
[5] Zakona o policijskim službenicima Kantona Sarajevo („Službene novine Kantona Sarajevo“ broj: 38/18)
[6] POLICIJSKI ETIČKI KODEKS ZA POLICIJSKE SLUŽBENIKE UPRAVE POLICIJE MINISTARSTVA UNUTRAŠNJIH POSLOVA KANTONA SARAJEVO, dostupno na: https://mup.ks.gov.ba/sites/mup.ks.gov.ba/files/policijski_eticki_kodeks.pdf (20.7.2022.);
[7] *Ibidem*;

4 promicati dobre odnose policije i građana, učinkovitu suradnju s drugim službama, lokalnim zajednicama i nevladinim organizacijama

## 3.2. Pravila ponašanja u policijskom postupanju

Od policijskih službenika javnost s pravom očekuje zakonitost, profesionalnost, poštenje i nepristranost. Za očuvanje povjerenja javnosti važno je otkloniti svaku sumnju da iza postupanja policijskih službenika stoje drugi motivi, kao i primjenjivati pravila ponašanja definirana Kodeksom za vrijeme i izvan radnog vremena. Pravila ponašanja u Kodeksu propisana su kroz sljedeće dijelove:[8]

1 Odgovornost policijskih službenika u poštivanju odredaba zakona i Kodeksa,
2 2 Odnosi s građanima i zadaće policijskih službenika,
3 Međusobni odnosi u Ravnateljstvu policije,
4 Odnosi s pripadnicima drugih agencija za provođenje zakona,
5 Smjernice za postupanje policijskih službenika prilikom poduzimanja službenih radnji,
6 Obrazovanje i stručno usavršavanje,
7 Primanje darova, gostoprimstva i drugih pogodnosti,
8 Nepristranost, izbjegavanje sukoba interesa i nespojivosti dužnosti s dužnostima policijskih službenika,
9 Ponašanje u vezi sa sredstvima,
10 Povjerljivost i korištenje službenih podataka
11 Radno okruženje.

[8] POLICIJSKI ETIČKI KODEKS ZA POLICIJSKE SLUŽBENIKE UPRAVE POLICIJE MINISTARSTVA UNUTRAŠNJIH POSLOVA KANTONA SARAJEVO, dostupno na: https://mup.ks.gov.ba/sites/mup.ks.gov.ba/files/policijski_eticki_kodeks.pdf (20.7.2022.);

### 3.2.1. Odgovornost policijskih službenika u poštivanju odredaba zakona i Kodeksa

Policijski službenici dužni su se pridržavati zakona i Kodeksa, dužni su se ponašati na visokom nivou tijekom i izvan radnog vremena te svojim ponašanjem ne štetiti ugledu Policijske uprave. Kodeks postavlja temeljne okvire pravila ponašanja pri obavljanju službenih dužnosti i utvrđuje vrijednosti kojih se treba pridržavati.

Policijski službenici trebaju biti u stanju pokazati dobru prosudbu, otvorenost, zrelost, poštenje, komunikaciju i, gdje je potrebno, vještine vođenja i upravljanja. Osim toga, trebali bi pokazati dobro razumijevanje društvenih i kulturnih pitanja, kao i pitanja lokalne zajednice. Poštivanje pravila definiranih Kodeksom ostvaruje se primjenom važećih zakonskih i podzakonskih akata.[9]

Policijski službenici imaju osobnu odgovornost za poštivanje zakona i Kodeksa i od njih se očekuje da će:[10]

1 1 obavljati dužnosti pažljivo, marljivo, profesionalno, s integritetom i nepristrano,
2 koristiti radno vrijeme produktivno iu skladu s dodijeljenim poslovima i zadaćama te za izvršavanje dodijeljenih zadataka,
3 pridržavati se najviših profesionalnih i etičkih standarda i nastojati postići više od minimalno očekivanog, u okviru očekivanih rezultata,
4 se upoznati s Kodeksom i postavljenim pravilima, a potpisom na Obrascu broj 1 koji je sastavni dio ovog Kodeksa policijski službenik potvrđuje da je pročitao, razumio i prihvatio Kodeks s pravilima koja su njime utvrđena,
5 pridržavati se važećih zakona i podzakonskih akata,
6 prema kolegama i građanima postupati ljubazno te voditi računa o njihovim pravima i obvezama te poštivati njihovu osobnost,
7 izbjegavati nepotrebno i prekomjerno trošenje i korištenje povjerenih sredstava,

[9] POLICIJSKI ETIČKI KODEKS ZA POLICIJSKE SLUŽBENIKE UPRAVE POLICIJE MINISTARSTVA UNUTRAŠNJIH POSLOVA KANTONA SARAJEVO, dostupno na: https://mup.ks.gov.ba/sites/mup.ks.gov.ba/files/policijski_eticki_kodeks.pdf (22.7.2022.);
[10] Ibidem;

8 čuvati službene i zaštićene podatke, kao i ne pribavljati niti tražiti protupravnu korist u svezi s bilo kojim službenim podatkom dobivenim u radu iu vezi s radom

9 ponašati se na način da potiče i povećava profesionalni i svaki drugi ugled Policijske uprave.

U obavljanju poslova policijski službenici dužni su poštivati i štititi ljudsko dostojanstvo i ljudska prava građana. Svi građani će biti tretirani jednako i djelovati isključivo na profesionalnoj osnovi, ne zastupajući, štiteći ili podrivajući interese bilo koje političke stranke, registrirane organizacije ili udruge, bilo kojeg konstitutivnog ili drugog naroda u Bosni i Hercegovini.[11]

#### *3.2.1.1. Poštenje u postupanju policijskih službenika*

Poštenje je temeljna osobina koja karakterizira osobnost policijskog službenika koji treba pokazati poštenje u svom radu, u odnosu prema građanima, kolegama, rukovoditeljima i drugim zaposlenicima. Prema službenim dokumentima i evidencijama Ravnateljstva policije i drugih agencija, policijski službenici postupaju s dužnom pažnjom, zakonito, istinito i točno popunjavaju evidencije, uključujući sve vrste obrazaca za potrebe kadrovske službe, kao i obrasce koji se odnose na na raspolaganje povjerenim sredstvima.

Ako policijski službenik prima naknadu ili dio naknade za koji zna ili misli da mu ne pripada, a odnosi se na rad u Ravnateljstvu policije, kao i u slučaju da uoči greške u obračunu svoje plaće, dužan je odmah izvijestiti Odjel za materijalno-financijske poslove Uprave policije.[12]

[11] *Ibidem*;
[12] *Ibidem*;

### *3.2.1.2. Kazneni, interni, prekršajni i disciplinski postupak*

Policijski službenici u obavljanju službene dužnosti, kao i u privatnom životu, moraju se ponašati u skladu sa zakonom. Pokretanje kaznene istrage, podizanje optužnice, a posebno potvrđivanje optužnice u kaznenom postupku, te pokretanje internog ili stegovnog postupka protiv policijskih službenika može dovesti do privremenog udaljenja od poslova i zadataka koje obavlja policijski službenik. policajac.

Zbog toga Policijska uprava i policijski službenici imaju posebnu odgovornost u primjeni zakona, zbog čega je nepoštivanje odredbi zakona od strane policijskih službenika i Policijske uprave vrlo ozbiljan problem.

Protiv policijskog službenika za kojeg postoji osnova sumnje da je počinio kazneno djelo provest će se interni postupak sukladno zakonskim i podzakonskim aktima kojima se uređuje interni postupak i stegovna odgovornost, neovisno o ishodu kaznenog postupka.

Policijski službenici će o svim kaznenim, kao i eventualnim prekršajnim postupcima koji se vode protiv njih, pravovremeno obavještavati neposrednog rukovoditelja. U izjavi koja se nalazi na Obrascu broj 2 (Prilog A2)[13], koji je sastavni dio ovog Kodeksa, policijski službenik navodi sve kaznene sankcije koje su mu izrečene, osim onih koje su brisane iz evidencije i prometnih prekršaja. .

Policijski službenik ne smije koristiti svoj službeni položaj ili odnose uspostavljene tijekom obavljanja službene dužnosti kako bi neprimjereno utjecao ili se miješao u istragu koju provodi Ravnateljstvo policije, druga agencija ili nadležno tijelo.[14]

[13] POLICIJSKI ETIČKI KODEKS ZA POLICIJSKE SLUŽBENIKE UPRAVE POLICIJE MINISTARSTVA UNUTRAŠNJIH POSLOVA KANTONA SARAJEVO, dostupno na: https://mup.ks.gov.ba/sites/mup.ks.gov.ba/files/policijski_eticki_kodeks.pdf (22.7.2022.);
[14] *Ibidem*;

#### *3.2.1.3. Ostale odgovornosti policijskih službenika*

Policijski službenik mora o svakom saznanju da je počinjena povreda službene dužnosti ili da ponašanje bilo kojeg zaposlenog u Upravi policije ima obilježja kriviČnog djela, takvu informaciju, bez odlaganja, proslijediti neposrednom starješini ili Odjeljenju za unutrašnju kontrolu Jedinice za profesionalne standarde.[15]

### 3.2.2. Odnosi s građanima i zadatci policijskih službenika

Građani očekuju da će postupak ostvarivanja njihovih prava i obveza u Policijskoj upravi biti zakonit, pošten, profesionalan i povjerljiv. Kako bi se osigurao visok standard ponašanja, potrebno je zauzeti pristojan i profesionalan odnos u ophođenju s građanima.[16]

Policijski službenici su u izvršavanju dužnosti obavezni da se ponašaju zakonito, pravično, ljubazno i pažljivo. Također, dužni su građanima pružiti svu moguću pomoć da ispune svoje obaveze i ostvare prava koja im po zakonu pripadaju.

Glavni ciljevi policije u demokratskom pravnom društvu su: očuvanje javnog reda i mira i provođenje zakona u društvu, zaštita i poštivanje temeljnih osobnih prava i sloboda, posebice sadržanih u Europskoj konvenciji o ljudskim pravima, sprječavanje, otkrivanje i suzbijanje kriminala i pružanje pomoći i uslužnih funkcija građanima.[17]

[15] POLICIJSKI ETIČKI KODEKS ZA POLICIJSKE SLUŽBENIKE UPRAVE POLICIJE MINISTARSTVA UNUTRAŠNJIH POSLOVA KANTONA SARAJEVO, dostupno na: https://mup.ks.gov.ba/sites/mup.ks.gov.ba/files/policijski_eticki_kodeks.pdf (22.7.2022.);
[16] *Ibidem*;
[17] *Ibidem*;

#### *3.2.2.1. Identifikacija policijskog službenika*

Policijski službenici dužni su se predstavljati u usmenoj, pisanoj i telefonskoj komunikaciji. U neposrednom kontaktu s građanima, prilikom obavljanja službenih radnji, policijski službenici dužni su imati službenu iskaznicu i policijsku značku kojom će se, po potrebi i na zahtjev građana, legitimirati.

Jedina iznimka od spomenutih pravila je kada se pokazivanjem službene iskaznice i policijske značke može ugroziti osobna sigurnost ili kada je od strane rukovoditelja dano posebno ovlaštenje da se ne nosi službena iskaznica i policijska značka zbog određenih okolnosti vezanih za službene poslove i zadatke.[18]

### 3.2.3. Međusobni odnosi policijskih službenika prilikom obavljanja dužnosti

Policijski službenici su dužni da stalno izgrađuju i unapređuju međusobno povjerenje i stvaraju dobre međuljudske odnose.

Razgovor između policijskih službenika treba da se vodi na način da odražava pravilan međusobni odnos i da ne vrijeđa ničije dostojanstvo. Službeni razgovori se obavljaju glasom normalne jačine i ne smiju se voditi u prisustvu nepoznatih lica. Policijski službenici su dužni da se međusobno oslovljavaju sa "Vi" i "Gospodine", "Gospođo" ili "Gospođice", uz obavezno navođenje funkcije-dužnosti koju obavljaju u Upravi policije ili drugoj Agenciji. Takođe, policijski službenici mogu se međusobno oslovljavati i sa "Kolega" odnosno "Kolegica", kada postoji obostrana saglasnost da se mogu oslovljavati i na "Ti".[19]

[18] *Ibidem*;
[19] *Ibidem*;

## 3.3. Smjernice postupanja policijskih službenika prilikom poduzimanja službenih radnji

Policijski službenici moraju poštivati svačije pravo na život kroz sve policijske aktivnosti. Policijski službenici ni pod kojim okolnostima neće počiniti, izazvati ili tolerirati bilo kakav čin mučenja ili nečovječnog i ponižavajućeg postupanja ili kažnjavanja. Policijski službenici mogu upotrijebiti silu kada je to potrebno i samo u mjeri potrebnoj za postizanje legitimnog cilja. Policijski službenici moraju uvijek provjeravati zakonitost službenih radnji koje namjeravaju poduzeti.

Policijski službenici izvršavat će propisno izdane zapovijedi svojih nadređenih, ali će imati obvezu suzdržati se od provođenja zapovijedi koje su očito nezakonite te će imati obvezu prijaviti takve zapovijedi bez straha od sankcija.[20]

Policijski službenici će svoje zadaće izvršavati pošteno, osobito vodeći se načelima nepristranosti i nediskriminacije. Policijski službenici će se miješati u pravo pojedinca na privatnost samo kada je to nužno i radi ostvarivanja legitimnog cilja.

Prikupljanje, čuvanje i korištenje osobnih podataka od strane policije provodit će se sukladno važećim odredbama Zakona o zaštiti osobnih podataka[21], kao i njegovim mogućim izmjenama i dopunama, zatim međunarodnim načelima zaštite osobnih podataka (Preporuka Vijeća Europe broj R (87)15 Odbora i dr.) te će se posebno ograničiti u mjeri potrebnoj za postići legitimne, utemeljene i specifične ciljeve i svrhe.[22]

Policijski službenici će u obavljanju svojih poslova uvijek imati na umu osnovna ljudska prava, kao što su sloboda misli, savjesti, vjere, izražavanja mišljenja, mirnog okupljanja, kretanja i nesmetanog uživanja imovine. Policijski službenici će postupati s integritetom i poštovanjem

[20] POLICIJSKI ETIČKI KODEKS ZA POLICIJSKE SLUŽBENIKE UPRAVE POLICIJE MINISTARSTVA UNUTRAŠNJIH POSLOVA KANTONA SARAJEVO, dostupno na: https://mup.ks.gov.ba/sites/mup.ks.gov.ba/files/policijski_eticki_kodeks.pdf (25.7.2022.);
[21] *Zakon o zaštiti osobnih podataka*, („Službeni glasnik Bosne i Hercegovine“, broj 49/06, 76/11 i 89/11), dostupno na: https://fzs.ba/wp-content/uploads/2016/06/zakon_podaci.pdf (25.7.2022.);
[22] POLICIJSKI ETIČKI KODEKS ZA POLICIJSKE SLUŽBENIKE UPRAVE POLICIJE MINISTARSTVA UNUTRAŠNJIH POSLOVA KANTONA SARAJEVO, dostupno na: https://mup.ks.gov.ba/sites/mup.ks.gov.ba/files/policijski_eticki_kodeks.pdf (26.7.2022.);

prema građanima te s posebnim osvrtom na položaj pojedinaca koji pripadaju posebno osjetljivim skupinama. Policijski službenici će tijekom intervencije biti u mogućnosti dokazati svoj policijski status i službeni identitet. Policajci će se suprotstaviti svim oblicima korupcije u policiji. O svakoj mogućoj korupciji obavijestit će svoje nadređene i druga nadležna tijela.[23]

## 3.4. Zaštita tajnosti podataka u postupanju policijskih službenika

Policijska uprava izražava punu spremnost da javnosti pruži objektivne informacije o svojim aktivnostima, bez otkrivanja povjerljivih podataka, odnosno podataka označenih stupnjem tajnosti. Policijski službenik ne smije bez odgovarajućeg ovlaštenja iznositi podatke do kojih je došao u obavljanju poslova. Ovo se pravilo odnosi na sve dokumente, zapise i elektronički pohranjene informacije. Također, policijski službenici dužni su štititi privatnost građana.

Načini na koje se službene informacije mogu zlouporabiti su:

1 otkrivanje informacija,
2 korištenje informacija za osobnu korist,
3 korištenje informacija u korist pojedinaca ili poslovnih subjekata i postizanje nezakonitih ciljeva,
4 korištenje određenih informacija dobivenih iz povjerljivih zapisa za zadovoljenje osobnih interesa ili interesa trećih strana i
5 brisanje, izmjena ili uništenje službene evidencije.

Strogo je zabranjeno poduzimanje bilo koje od prethodno navedenih radnji i kao i drugih radnji koje predstavljaju neovlašteno korištenje povjerljivih službenih podataka.[24]

[23] *Ibidem*;
[24] *Ibidem*;

### 3.4.1. Diskrecija – zaštita tajnosti podataka

Policijski službenik ne smije sudjelovati u izradi znanstvenih ili stručnih radova ili istraživačkih projekata koji sadrže stavove ili mišljenja o političkim pitanjima, ako se stavovi i mišljenja izraženi u tim radovima mogu eksplicitno ili implicitno shvatiti kao stavovi i mišljenja Policijske uprave. Trebalo bi se suzdržati od davanja neprikladnih javnih komentara, a posebno:

1 komentare i izražavanje negativnog mišljenja o politici institucija Bosne i Hercegovine, entiteta, kantona i Brčko Distrikta BiH,
2 daje primjedbe na programe u čijoj izradi ili provedbi sudjeluje i policijski službenik,
3 izjave ili mišljenja koja bi se mogla tumačiti kao službeni komentari i
4 kritike načina vođenja Policijske uprave u cjelini i rada njezina vodstva.

Sudjelovanje u anonimnim anketama u kojima se od policijskih službenika traži da izraze svoje mišljenje o gore navedenim pitanjima neće se smatrati povredom diskrecijskog prava.[25]

#### *3.4.1.1. Odnosi s javnošću i tajnost podataka*

Samo ovlašteni policijski službenici mogu komunicirati s medijima i govoriti u ime Ravnateljstva policije o poslovima iz djelokruga Ravnateljstva policije. Policijski službenici ovlašteni za komuniciranje s javnošću dužni su postupati pažljivo i pravodobno, jedinstveno i koordinirano prosljeđivati točne podatke i jasne poruke. Policijski službenik ne smije se upuštati u razgovor s predstavnicima medija o pitanjima koja se odnose na rad policijskog službenika bez odobrenja načelnika Ravnateljstva policije ili druge ovlaštene osobe koja, ako je to potrebno, komunicira s javnost, pružit će mu podršku u vezi s tim.

Interes javnosti za osobne prilike policijskog službenika ponekad može utjecati na rad Policijske uprave. Ukoliko se policijski službenik nađe u takvoj situaciji, odmah će o tome u što

[25] POLICIJSKI ETIČKI KODEKS ZA POLICIJSKE SLUŽBENIKE UPRAVE POLICIJE MINISTARSTVA UNUTRAŠNJIH POSLOVA KANTONA SARAJEVO, dostupno na: https://mup.ks.gov.ba/sites/mup.ks.gov.ba/files/policijski_eticki_kodeks.pdf (27.7.2022.);

kraćem roku obavijestiti svog neposrednog rukovoditelja. Policijski službenik nikada i ni pod kojim uvjetima u situacijama iz ovoga članka ne smije odati podatke koji predstavljaju tajne podatke.[26]

#### *3.4.1.2. Obraćanje javnosti – korištenje službenih informacija*

Ukoliko je policijski službenik u situaciji da pred određenom skupinom govori ili izlaže u ime Policijske uprave (predavanja, sudjelovanje na seminarima i sličnim skupovima), au tu svrhu treba koristiti službene podatke ili iskustvo, dužan je pribaviti odobrenje načelnika Policijske uprave. Prije dobivanja odobrenja za sudjelovanje na službenim skupovima u ime Policijske uprave, policijski službenik će sadržaj govora ili predavanja izložiti načelniku Policijske uprave. Odobrenje će se izdati ako načelnik Policijske uprave ocijeni ili odobri da je takav govor ili predavanje u skladu s ciljevima i politikama Policijske uprave.

Ako policijski službenik želi održati govor u organizaciji ili drugom skupu koji nije vezan za njegovo svojstvo zaposlenika Ravnateljstva policije u čijem radu osobno sudjeluje, te ako tom prilikom treba koristiti službenu informacija ili iskustva, mora zatražiti odobrenje od načelnika Policijske uprave. Odobrenje će se izdati pod sljedećim uvjetima:

1 da se govor održi izvan službenog radnog vremena,
2 ne zahtijevati korištenje sredstava od Policijske uprave i
3 da su podaci podobni za objavu, da su točni i da odražavaju politiku Policijske uprave.

Policijski službenik nikada, ni pod kojim uvjetima, u takvim situacijama ne smije odati podatke koji predstavljaju tajne podatke.[27]

[26] POLICIJSKI ETIČKI KODEKS ZA POLICIJSKE SLUŽBENIKE UPRAVE POLICIJE MINISTARSTVA UNUTRAŠNJIH POSLOVA KANTONA SARAJEVO, dostupno na: https://mup.ks.gov.ba/sites/mup.ks.gov.ba/files/policijski_eticki_kodeks.pdf (27.7.2022.);
[27] POLICIJSKI ETIČKI KODEKS ZA POLICIJSKE SLUŽBENIKE UPRAVE POLICIJE MINISTARSTVA UNUTRAŠNJIH POSLOVA KANTONA SARAJEVO, dostupno na: https://mup.ks.gov.ba/sites/mup.ks.gov.ba/files/policijski_eticki_kodeks.pdf (28.7.2022.);

# 4. INFORMACIJSKA SIGURNOST

## 4.2. Sigurnost

Pojam sigurnosti potječe od latinske riječi „ *securitas*“ što znači sigurnost, odnosno siguran, pouzdan, zastićen. Riječ je o pojmu koji ima negativan aspekt određenja, te je stoga za potvrdnu definiciju potrebno analizirati niz sustavskih pitanja.[28]

Teorijski gledano, sigurnost predstavlja apsolutan pojam, što znaši da je netko ili nešto sigurno ili nesigurno. Međutim, u stvarnom okruženju, sigurnost nije apsolutna kategorija nego bi se prije moglo govoriti kako joj je svojstven određen stupanj relativiteta.

Apsolutne sigurnosti nema nigdje ali je važno da se postigne i odrzava stupanj sigurnosti koji ljudima osigurava normalan život i rad. Pojam sigurnosti se koristi u društvenim naukama u različitom kontekstu od nacionalne sigurnosti, socijalne, pravne do sigurnosti na radu. Sigurnost jedan od temeljnih fenomena ljudskog društva u svim fazama njegovog razvoja. Bez obzira je li riječ o sigurnosti pojedinca, države, skupine država ili međunarodne zajednice uvijek se radi o nastojanju da se osiguraju vrijednosti i stanje za koje se smatra da su od vitalnog značaja.[29]

Možemo objasniti četiri temeljna, odnosno osnovna pristupa proučavanja pojma sigurnosti. Tako da imamo četiri vrste sigurnosti:[30]

1 Proučavanje sigurnosti na nivou nacionalne države, koji se odnosi na probleme sigurnosti i opstanka pojedine države – nacionalna sigurnost
2 Sigurnost na međunarodnom nivou kao temeljne instrumente za ostvarivanje međunarodne sigurnosti – međunarodna sigurnost
3 Regionalni pristup koji je usmjeren na proučavanje sigurnosne problematike u pojedinim svjetskim regijama – regionalna sigurnost

[28] Čizmić J., Boban M., Zlatović D., *Nove tehnologije, intelektualno vlasništvo i informacijska sigurnost*. Split: Sveučilište u Splitu Pravni fakultet, 2016.;
[29] Tatalovic S., Bilandzic M., (2011.), *Osnove nacionalne sigurnosti* str. 23.;
[30] Dimitrijević, Vojin (1973.) *Pojam sigurnosti u međunarodnim odnosima*. Beograd: Savremena administracija;

4 Globalni pristup obuhvata pojam sigurnosti cjelovitu u sadržajnom i prostornom smislu – globalna sigurnost

Iz razloga jer se uz pojam sigurnosti vezuje pojam nacionalne sigurnosti, u daljnjem tekstu je detaljnije prikazan i objašnjen pojam nacionalne sigurnosti.[31]

### 4.2.1. Sigurnosne prijetnje

Opasnosti koje prijete sigurnosti država su promjenljive veličine, te je većina definicija podložna stalnom istraživanju temeljnih interesa i vrijednosti države te njezinih odgovora na te izazove. Kod primjera malih zemalja nacionalna sigurnost se uglavnom ograničava na zaštitu od stvarnog ili potencijalnog napada, a rastom veličine zemlje po pravilu se proširuju i granice nacionalnih interesa i ciljeva koje treba štititi.[32]

Jedna od najvećih opasnosti koje prijete sigurnosti jeste vojni poraz. u oružanom sukobu, pa se često pogrešno nacionalna sigurnost ograničava samo na vojno-stratešku sigurnost, a rješenje problema traži gomilanjem vojne sile (moći) .

Izvori ugrožavanja nacionalnih interesa mogu biti vanjski i unutrašnji, a mogu imati sljedeće oblike[33]:

1 pokušaji dovođenja nacije u podređeni položaj ili ovisnost o drugoj državi ili međunarodnoj organizaciji
2 podrivanje ili slabljenje nacionalne obrambene i vojne moći
3 podrivanje ili slabljenje nacionalne gospodarske i financijske moći
4 napad na objekte vitalne infrastrukture te javne i zaštićene komunikacijske sustave
5 odavanje klasificiranih podataka
6 velike prirodne i civilne katastrofe

[31] Rhodes-Ousley M., *Information Security*: *The Complete Reference, Second Edition, McGraw Hill Professional*, 2013.;
[32] Čizmić J., Boban M., Zlatović D., *Nove tehnologije, intelektualno vlasništvo i informacijska sigurnost*. Split: Sveučilište u Splitu Pravni fakultet, 2016.;
[33] *Ibidem*;

7 epidemije
8 djela koja su zabranjena međunarodnim pravom kao što je nedopuštena trgovina oružjem, drogom i ljudima,
9 oružani napad odnosno agresija od strane druge ili drugih država
10 unutarnja oružana pobuna
11 terorizam
12 diverzije
13 špijunaža
14 otmice i uzimanje talaca
15 politički motivirano nasilje
16 nasilno izdvajanje državnog područja ili pripojenje državnog područja drugoj državi
17 nasilna promjena ustavnog i zakonskog poretka ili sprječavanje njihove uspostave, uključujući državni/vojni udar
18 izvanjsko tajno nastojanje za ostvarivanje utjecaja na nacionalne političke i gospodarske odnose i tijekove.

Organi za održavanje nacionalne sigurnosti unutar FBiH su državni organi, odnosno konkretno u slučaju Bosne i Hercegovije je to Ministarstvo sigurnosti, a ono je nadležno za poslove:[34]

1 zaštite međunarodnih granica, unutrašnjih graničnih prijelaza i reguliranje prometa na graničnim prijelazima Bosne i Hercegovine;
2 sprječavanja i otkrivanja počinitelja kaznenih djela terorizma, trgovine drogom, krivotvorenja domaće i strane valute i trgovine ljudima i drugih kaznenih djela s međunarodnim ili međuentitetskim elementom;
3 međunarodnu suradnju u svim oblastima iz nadležnosti Ministarstva (npr., suradnja s INTERPOL-om, EUROPOL-om, SELEC, MARRI…);
4 organizaciju i usuglašavanje aktivnosti entitetskih ministarstava unutrašnjih poslova i Brčko Distrikta BiH u ostvarivanju sigurnosnih zadataka u interesu Bosne i Hercegovine;

[34] Miletić, Andreja (1978.) *Nacionalni interes u američkoj teoriji međunarodnih odnosa*. Sarajevo - Beograd: Savremena administracija;

5 Uređuje procedure i način organizacije službe vezano za kretanje i boravak stranaca u Bosni i Hercegovini;

6 forenzička ispitivanja i vještačenja.

U okviru ovog ministarstva (BiH), kao upravne organizacije su formirani Direkcija za koordinaciju policijskih tijela BiH, Državna agencija za istrage i zaštitu, Granična policija BiH, Agencija za školovanje i stručno usavršavanje kadrova, Agencija za forenzička ispitivanja i vještačenja, Agencija za policijsku podršku i Služba za poslove sa strancima.[35]

## 4.2.2. Informacijska sigurnost i suvremena tehnologija

### *4.2.2.1. Informacijski prostor*

Informacijski prostor predstavlja virtualnu globalnu okolinu međusobno povezanih javnih i privatnih informacijski 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.[36]

Slijedom prethodno navedenog 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

[35] *Ibidem*;
[36] Rhodes-Ousley M., *Information Security*: *The Complete Reference, Second Edition, McGraw Hill Professional*, 2013.;

posljednjih nekoliko desetljeća mogu se utvrditi neke karakteristične faze kroz koje je oblikovanje javnog informacijskog prostora prolazilo.[37]

Informacija prestavlja izvor rukovođenja, u obliku kapitala i rada, te predstavlja jednu od najznačajnijih upotreba informacijske tehnologije kao konkurentskog oružja. Kao resurs ima posebna obilježja jer za razliku od materije i energije ne troši se korištenjem, niti smanjuje raspodjelom. Informacija se danas nalazi u središtu poslovanja i predstavlja njen centralni faktor.

Dominacija informacijske funkcije ukazuje s jedne strane na potrebu informatizacije poslovanja unutar poslovnog sustava, a s druge strane na efikasno povezivanje s izvorima informacija iz njene okoline što tom okruženju osigurava uspješno poslovanje i izglednu budućnost. Jedino oni poslovni sustavi koji polažu dovoljno pažnje razvoju informacijskog sustava mogu se nositi sa složenim uvjetima svjetskog tržišta i konkurencije.[38]

Informacijski sustav poslovnog sustava izuzetno je značajan za njegovu opstojnost i poslovanje, stoga je njegovo strateško planiranje jednako važno koliko i strateško planiranje poslovnog sustava. Cilj informacijskog sustava je dostaviti pravu informaciju na pravo mjesto, u pravo vrijeme i uz minimalne troškove. Osnovne zadaće informacijskog sustava su: prikupljanje, razvrstavanje, obrada, čuvanje, oblikovanje i raspoređivanje informacija na sve razine objektnog sustava, odnosno korisnicima.[39]

Informacijski sustav označava skup kvalitetno oblikovanih pravila, običaja i postupaka pomoću kojih ljudi, oprema ili kombinacija tog dvoga, djeluju sa svrhom da dobiju informacije koje će zadovoljiti potrebe određenih pojedinaca u određenoj poslovnoj situaciji. [40]

[37] Klaić A., Perešin A.: *Zbornik radova*; Dani kriznog upravljanja 2011. 678-708 str. Veleučilište Velika Gorica 2011.
[38] Čizmić J., Boban M., Zlatović D., *Nove tehnologije, intelektualno vlasništvo i informacijska sigurnost*. Split: Sveučilište u Splitu Pravni fakultet, 2016.;

[39] Luić Lj.: *Informacijski sustavi*, Veleučilište u Karlovcu, Karlovac 2009; str.36.;
[40] Šehanović J. i dr.: *Informatika za ekonomiste*, Sveučilište u Rijeci, Pula 2002., str. 50.;

#### *4.2.2.2. Suvremene prijetnje informacijskoj sigurnosti*

Sigurnost informacijskih sustava bitna je tema kojoj organizacije diljem svijeta pridaju mnogo pažnje za što postoji i dobar razlog. Sigurnosne prijetnje dolaze iz više izvora poput računalnog kriminala, špijunaže, sabotaža i prirodnih nepogoda.[41]

Šteta počinjena od strane računalnog kriminala sve je veća što pokazuju financijski pokazatelji pa je bitno definirati, planirati, projektirati, implementirati, održavati i kontinuirano poboljšavati informacijsku sigurnost. Područja informacijske sigurnosti za koja se propisuju mjere i standardi informacijske sigurnosti su:[42]

1 sigurnosna provjera,
2 fizička sigurnost,
3 sigurnost podatka,
4 sigurnost informacijskog sustava,
5 sigurnost poslovne suradnje.

Informacijska sigurnost označava stanje povjerljivosti, cjelovitosti i raspoloživosti podatka, koje se postiže primjenom propisanih mjera i standarda informacijske sigurnosti te organizacijskom podrškom za poslove planiranja, provedbe, provjere i dorade mjera i standarda.[43]

Pored zakona informacijska sigurnost definirana je i ISO 27001 standardom:[44] Informacijska sigurnost podrazumijeva očuvanje povjerljivosti, integriteta i dostupnosti informacije; uključiti se mogu i druge osobine kao što su vjerodostojnost, odgovornost, neporecivost i pouzdanost. Uz ovaj pojam ISO 27001 definira sljedeće pojmove bitne za ovo područje:[45]

[41] Čizmić J., Boban M., Zlatović D., *Nove tehnologije, intelektualno vlasništvo i informacijska sigurnost*. Split: Sveučilište u Splitu Pravni fakultet, 2016.;
[42] *Zakon o informacijskoj sigurnosti*, NN 79/07;
[43] Kostanjevec A. i dr.. *Sigurnost informacijskih sustava verzija* 01012014, FOI Varaždin 2014. str.2.;
[44] *Ibidem*;
[45] *Ibidem*;

- sigurnosni događaj – prepoznatljiv slučaj stanja sustava, usluge ili mreže koji upućuje na moguću povredu politike informacijske sigurnosti ili neuspjeh zaštite ili do tada nepoznate okolnosti koje mogu biti važne za sigurnost;[46]
- sigurnosni incident – naznačen jednim ili nizom neželjenih ili neočekivanih sigurnosnih događaja koji imaju značajnu vjerojatnost ugrožavanja poslovnih aktivnosti i informacijske sigurnosti;
- zaštita – nositelja svih informacija potrebnih za nesmetan rad poslovnog sustava. Zaštita podrazumijeva provođenje mjera poradi osiguranja informacijskog sustava;
- ranjivost – s obzirom na to da je sustav ranjiv, pa tako postoji rizik da informacija bude izložena neovlaštenom pristupu. ISO 27002 ranjivost definira kao:[47] „Ranjivost je slabost imovine ili grupe imovina koju jedna ili više prijetnji mogu iskoristiti.“ Općenito možemo ranjivosti podijeliti na ranjivosti aplikacije i ranjivosti operacijskog sustava.[48]
- rizik – ISO 27001 pri opisu upravljanja informacijskom sigurnošću ISMS navodi kako je dio cjelokupnog sustava upravljanjem, temeljen na pristupu sa strane poslovnih rizika, kako bi uspostavio, implementirao, nadzirao, provjeravao, održavao i unapređivao informacijsku sigurnost. Rizik je u knjigama opisan kao funkcija razine prijetnje, ranjivosti i vrijednosti informacijske imovine. izik se jasnije može opisati kao vjerojatnost prijetnje da iskoristi neku ranjivost imovine te time ugrozi imovinu.[49]

### 4.2.3. Zaštita sigurnosti podataka

Informacijski sustav je dio skoro svakog poslovnog sustava, neovisno koju vrstu poslovnih procesa podržava ili veličini organizacije u kojoj funkcionira, IS je ključni element poslovanja. Podrazumijeva se da je njegova uloga, također i važnost popraćena galopirajućim rastom i

[46] Čizmić J., Boban M., Zlatović D., *Nove tehnologije, intelektualno vlasništvo i informacijska sigurnost*. Split: Sveučilište u Splitu Pravni fakultet, 2016.;
[47] Boban M, Perišić M., *Biometrija, Zbornik radova Veleučilišta u Šibeniku*, No.1-2/2015, srpanj 2015, str. 115-148.;
[48] *Ibidem*;
[49] *Ibidem*;

primjenom informacijske komunikacijske tehnologije (eng. *Information and Communication Technology* – ICT).

Cilj informacijskog sustava je prikupljanje, obrada, pohrana, čuvanje i distribucija informacija potrebnih pri izvođenju poslovnih procesa i upravljanju poslovnim sustavom. Uobičajeni su dijelovi IS-a sustav za obradu transakcija, upravljački izvještajni sustav, sustav za potporu i odlučivanje i sustav uredskog poslovanja. IS djeluje unutar poslovnom sustava, a na taj način omogućuje mu da je u interakciji sa internom i eksternom okolinom organizacije.[50]

Bitno je naglasiti i temeljne aktivnosti poslovnog sustava:[51]

1 izvršavanje poslovnih procesa, pri tom se misli na osnovnu djelatnost nekog poslovnog sustava, (neovisno o djelatnosti i veličini organizacije), odnosno sve one poslove koji se u njemu obavljaju (npr. nabava sirovine i energije, proizvodnja, daljnji plasman proizvoda, razne marketinške i financijske transakcije itd);
2 u pravljanje poslovnim sustavom, pri tom se misli na to kako svaki poslovni sustav (neovisno radi li se o državnim tijelima ili pravnoj osobi) nastoji izgraditi dobar informacijski sustav koji će dati podlogu za brzo i kvalitetno odlučivanje.

Navedene aktivnosti podupire neka vrsta informacijskog sustava. Efikasnost i djelovanje nekih poslovnih postupaka bili bi nezamislivi bez korištenja informacijsko komunikacijske tehnologije. Kako je već navedeno, IS se definira kao poslovnog sustava a čine ga potrebna infrastruktura, koju čine svi potrebni fi zički uređaji i oprema, kojim upravlja čovjek s ciljem što efikasnijeg izvršavanja poslovnih ciljeva. IS-e razlikujemo prema njihovoj kompleksnosti: na jednostavne, složene i inteligentne IS-e. Prema njihovom opsegu postoje: IS-e na razini društva, republike, županije, regije itd.[52]

[50] Čerić, V., Varga, M., 2004., *Informacijska tehnologija u poslovanju*, Sveučilište u Zagrebu, Element, Zagreb;
[51] Čizmić J., Boban M., Zlatović D., *Nove tehnologije, intelektualno vlasništvo i informacijska sigurnost*. Split: Sveučilište u Splitu Pravni fakultet, 2016.;
[52] *Ibidem*;

#### *4.2.3.1. Procjena rizika*

Prilikom procjene rizika uzima se u obzir poslovna strategija organizacije i njezini ciljevi. Kroz samu procjenu rizika identifi ciraju se moguće prijetnje imovini organizacije i stupanj ranjivosti. Također, određuje se i vjerojatnost pojava prijetnji i njihov utjecaj na rad organizacije te eventualnu procjenu štete.[53]

Sigurnosni rizik se definira kao mogućnost realizacije nekog neželjenog događaja. Neželjeni događaj može utjecati na:[54]

- povjerljivost (eng. *confi dentiality*) se odnosi na zaštitu određenih sadržaja, od bilo kakvog namjernog ili nenamjernog otkrivanja neovlaštenim osobama;
- integriteta (eng. *integrity*) - mora osigurati konzistentnost informacija i onemogućiti bilo kakve neovlaštene promjene sadržaja;
- raspoloživost (eng. availability) informacijskih resursa podrazumijeva da su sve relevantne informacije, u za to vremenski prihvatljivom terminu, raspoložive odgovarajućim (ovlaštenim) subjektima

Pod pojmom „*ranjivosti sustava*“ podrazumijevaju se svi propusti i slabosti sustava sigurnosti koji omogućuju provođenje eventualnih nedopuštenih aktivnosti. Ranjivosti sustava najčešće se povezuju s propustima programskog koda, no mogući su i mnogi drugi propusti kao što su propusti u dizajnu samog sustava, propusti u implementaciji i održavanju sustava, neprikladan odabir tehnologije i alata itd. Bez adekvatno provedene analize ranjivosti, skoro je nemoguće odrediti sigurnosni rizik. [55]

[53] Strenburner, G., Goguen, A., Feringa, A., *Risk Management Guide for Infromation Tehnology System*, NIS – National Institute of Standard and Tehnology, U.S. Department of Commerce, July 2002.
[54] *Ibidem*;
[55] *Ibidem*;

# 5. INFORMACIJSKA SIGURNOST U POLICIJSKIM POSTUPCIMA

Kibernetička sigurnost postaje sve aktuelnija tema u IT (informacijska tehnologija) i OT (telekomunikacijskih) sektorima. Uvođenjem interneta u većinu sustava i uređaja (tzv. *Internet of Things*, skraćeno IOT) postaju ICT (informacijska i komunikacijska tehnologija) sustavi sve napredniji i zastupljeniji. Napretkom informacijskih i komunikacijskih tehnologija i ostvarivanjem veza između IT i OT računalnih mreža, te korištenjem komercijalnih PC (Kompjutorskih) tehnologija u OT svijetu je dovelo do ugroze do tada sigurnih OT sustava.[56]

Putem interneta odnosno IOT, moguća su dva načina komunikacije u IT i OT sustavima: Uređaj – Čovijek; Čovijek – Uređaj.

Kibernetička sigurnost se tiče osiguravanja ranjivih stvari putem IT-a. To se odnosi na podatke koji se pohranjuju i tehnologije koje se koriste za njihovo osiguranje. Dio kibernetičke sigurnosti u vezi s zaštitom informacijskih i komunikacijskih tehnologija - tj. *hardver* i *softver* poznat je pod nazivom ICT sigurnost.

Sektori industrije ICS/OT i ICT/IT danas predstavljaju tehnološke grane koje sve više funkcioniraju u simbiozi, određene IT tehnologije imaju značajnu primjenu u industriji, a industrija pruža podršku IT sektoru tako što pruža potrebne energije putem primarnih i rezervnih izvora.

Navedeni integracijski procesi su neizbježni i predstavljaju evoluciju poslovanja. Aktivni pristup praćenju IT trendova, novi poslovni modeli i industrijske tehnologije preduvjet su za održivi razvoj i dugoročnu konkurentnost energetskih tvrtki.

[56] Čizmić J., Boban M., Zlatović D., *Nove tehnologije, intelektualno vlasništvo i informacijska sigurnost*. Split: Sveučilište u Splitu Pravni fakultet, 2016.;

Razvoj sigurnosti energetskog sustava predstavlja novi izazov za koji se očekuje da će porasti u skorijoj budućnosti. Radi se analiza trenutnog stanja i osnovno pojašnjenje kibernetičke sigurnosti industrije u skladu s novim propisima.[57]

## 5.1. Kibernetički prostor – sigurnost

Prijetnje dolaze nepostredno prije potencijalnog napada i ciljanog djelovanja da se našteti sigurnosti informacijskog sustava koji sadrži i podatke koji su povjerljivi ili tajni. Kada se radi o pojmu kibernetičkih ili *cyber* prijetnji, tada se podrazumijeva radnje opisane u nastavku.[58]

*Krađa identiteta* – Lažno predstavljanje je praksa slanja lažnih e-poruka koje nalikuju e-porukama iz uglednih izvora. Cilj je ukrasti osjetljive podatke poput brojeva kreditnih kartica i podataka o prijavi. To je najčešća vrsta kibernetičkih napada. Možete se zaštititi obrazovanjem ili tehnološkim rješenjem koje filtrira zlonamjerne e-poruke.

*Socijalni inžinjering* – Taktika koju protivnici koriste kako bi vas naveli na otkrivanje osjetljivih podataka. Oni mogu tražiti novčano plaćanje ili dobiti pristup vašim povjerljivim podacima. Društveni inženjering može se kombinirati s bilo kojom od gore navedenih prijetnji da biste imali veću vjerojatnost da ćete kliknuti na veze, preuzeti zlonamjerni softver ili vjerovati zlonamjernom izvoru.

*Ransomware* – vrsta zloćudnog softvera. Kreiran je za iznuđivanje novca blokiranjem pristupa datotekama ili računalnom sustavu dok otkupnina ne bude plaćena. Plaćanje otkupnine ne jamči vraćanje datoteka ili vraćanje sustava.

*Malware* – Zlonamjerni softver je vrsta softvera namijenjena za neovlašteni pristup ili oštećivanje računala.

[57] Strenburner, G., Goguen, A., Feringa, A., *Risk Management Guide for Infromation Tehnology System*, NIS – National Institute of Standard and Tehnology, U.S. Department of Commerce, July 2002
[58] Čizmić J., Boban M., Zlatović D., *Nove tehnologije, intelektualno vlasništvo i informacijska sigurnost*. Split: Sveučilište u Splitu Pravni fakultet, 2016.;

*Malware na mobilnim aplikacijama* – Mobilni uređaji ranjivi su na napade malware-a baš kao i ostali računalni hardver. Napadači mogu ugraditi zlonamjerni softver u preuzimanja aplikacija, mobilne web stranice ili e-poštu i tekstualne poruke. Jednom kad je kompromitiran, mobilni uređaj zlonamjernom lopovu može omogućiti pristup osobnim podacima, podacima o lokaciji, financijskim računima i još mnogo toga.

*Prijetnje kroz IOT uređaje* – IOT uređaji poput industrijskih senzora ranjivi su na više vrsta kibernetičkih prijetnji. Uključuju hakere koji preuzimaju uređaj kako bi ga učinio dijelom DOS[59] napada i neovlašteni pristup podacima koje uređaj prikuplja. S obzirom na njihov broj, geografsku distribuciju i često zastarjele operativne sustave, IOT uređaji glavna su meta zlonamjernih aktera.

*Trojanci* – Nazvan po trojanskom konju drevne grčke povijesti, trojanac je vrsta zlonamjernog softvera koji ulazi u ciljni sustav izgledajući poput jedne stvari, npr. standardni dio softvera, ali zatim izdaje zlonamjerni kod – pin unutar glavnog sustava.

*Malvertising* - Zlonamjerno oglašavanje upotreba je mrežnog oglašavanja za širenje zlonamjernog softvera.

Kibernetički napadi se dijele u 4 skupine, odnosno kategorije, koje se ogledaju kroz:

1 *Kibernetički kriminal* – kriminal koji je izveden uz pomoć računala ili računalne tehnologije. Najčešće se ova kategorija povezuje s prijevarama koje uključuju internet bankarstvo i razne prijevare na web trgovinama upotrebom tuđih, nelegalno stečenih, kreditnih kartica. Smatra se da je kibernetički kriminal najbrže rastući sektor globalno organiziranog kriminala, ali pretpostavka je da će u budućnosti još više rasti. Razlog za to je što za bilo kakav napad tog oblika nije potrebna fizička prisutnost napadača. U današnje vrijeme moguće je ispaliti projektil, kupiti oružje, upasti u informacijske sustave

[59] Schwartz, P.M., „*The Computer in German and America Constitutional Law: Towards an American Right of Information Self-Determination*, American Journal of Comparative Law, 1989., vol. 37;

raznih državnih i nedržavnih institucija samo jednim klikom sa računala koje se ni ne nalazi u blizini mete.[60]

2 *Kibernetičku špijunažu* – akcija pomoću koje se stječu tajne informacije bez dopuštenja oštećene osobe. Najčešće se koristi u industriji kako bi se stekla prednost nad konkurencijom tako da se istraži proizvod koji će plasirati na tržište i pokuša napraviti jednak ili bolji proizvod prije negoli ga konkurencija stigne plasirati. Također, još jedna od najčešćih primjena kibernetičke špijunaže je u vojne svrhe. Razlog za to je što svaka zemlja želi biti najjača i želi znati čime raspolažu druge zemlje jer vojna nadmoć, nažalost, znači i nadmoć u svemu ostalom. Kibernetička špijunaža se izvodi pomoću špijunskih programa, računalnih virusa, trojanskih konja i raznim drugim načinima

3 *Kibernetički terorizam* – planirani i politički motivirani napadi koje najčešće izvode nacionalne skupine, rjeđe pojedinci. Jedna od stvari koje se svrstavaju u kibernetički terorizam je regrutiranje sljedbenika ISIL-a preko društvenih mreža na kojima dogovaraju i koordiniraju napadima. Za očekivati je da će i takav oblik terorizma evoluirati na način da će svaka od tih akcija putem računala imati ljudske žrtve kao posljedicu. Ako ne direktno, onda će kombinacija kibernetičkog i fizičkog terorizma uskoro biti vrlo ozbiljna tema rasprava zaštite nacionalne sigurnosti. Jedan primjer takve kombinacije je da se uslijed fizičkog čina terorizma, npr. autobombe, onemoguće komunikacijski sustavi kako pomoć ne bi stigla na vrijeme i to bi rezultiralo puno većim brojem ljudskih žrtava.[61]

4 *Kibernetički rat* – rat koji se vodi uz pomoć računala i računalnih mreža. Najčešće je barem jedan od sudionika država. Najjednostavnije objašnjenje kibernetičkog rata je da je to informacijski rat kojim se pokušava steći informacijska prednost nad protivnikom u ratu. Jedan od načina da se to postigne je krađa i izmjena protivničkih informacija. Kibernetički rat je zapravo događaj ili aktivnost u kojoj se kontinuirano i učestalo koristi

[60] K. Stouffer, S. Lightman, V. Pillitteri, M. Abrams, A. Hahn, *Guide to Industrial Control Systems (ICS) Security, NIST- National Institute of Standards and Technology*, Gaithersburg, Svibanj 2014., str. 155.;
[61] Čizmić J., Boban M., Zlatović D., *Nove tehnologije, intelektualno vlasništvo i informacijska sigurnost*. Split: Sveučilište u Splitu Pravni fakultet, 2016.;

kibernetički terorizam, kibernetičku špijunaži i kibernetički kriminal u svrhu napada na protivnika.[62]

Svaki od prethodno navedenih napada na informacijski sustav, samostalno može naštetiti informacijskom sustavu, te ugroziti informacijsku sigurnostu, a ujedno i smanjiti stupanj zaštite podataka.[63]

## 5.2. Zaštita informacija i podataka u informacijskom prostoru

Zaštita informacijskog sustava se može vršiti kroz tri postupka, a to su: fizičke, programske i organizacijske mjere zaštite. Provođenjem ovih mjera samostalno ili u međusobnoj kombinaciji, informacijski sustav, kao i podatci se mogu zaštititi od prijetnji i napada na iste. U nastavku su detaljnije opisanje mjere zaštite informcacijskog sustava i podataka.

### 5.2.1. Fizičke mjere zaštite

Fizičke metode zaštite jedna su od ključnih komponenti u cjelokupnoj zaštiti informacijskog sustava. Fizička sigurnost informacijskog sustava ugrožava se u slučajevima elementarnih nepogoda te ljudskih ranjivosti, kao što je sabotaža, krađa i neposlušnost.

Primjena fizičke sigurnosti podrazumijeva proces uporabe mjera zaštite kako bi se spriječio neovlašten pristup, oštećenje ili uništenje dobara.[64] Fizička sigurnost smatra se osnovom informacijske sigurnosti te su ostale sigurnosne mjere utemeljene upravo na njoj.[65]

---

[62] K. Stouffer, S. Lightman, V. Pillitteri, M. Abrams, A. Hahn, *Guide to Industrial Control Systems (ICS) Security, NIST- National Institute of Standards and Technology*, Gaithersburg, Svibanj 2014., str. 156.;
[63] *Ibidem*;
[64] *Informacijska sigurnost, zaštita podataka, osobnih podataka i informacija* http://www.cert.hr/sites/default/files/NCERT-PUBDOC-2010-06-304.pdf (28.7.2022.);
[65] Klasić, K., Klarin, K., *Informacijski sustavi : načela i praksa*.: Intus informatika, Zagreb 2009., str. 114. ;

### 5.2.2. Programske mjere zaštite tajnosti podataka u informacijskom sustavu

Kod pojma programskih mjera zaštite informacijske sigurnosti podataka, poznaju se dvije opcije koje se mogu primjeniti u ovom postupku, a to su zaštita na razini operacijskog sustava i zaštita na razini korisničkih programa.[66]

Zaštita na razini operacijskog sustava je osnovni stupanj zaštite. On uključuje administratore sustava i korisnike tj. zaposlenike u organizaciji. Administrator sustava ima pristup svim povlaštenim informacijama te dodjeljuje razinu ovlasti pojedinim korisnicima.

Administrator svakom korisniku određuje njegovo korisničko ime te lozinku kojima se koristi kako bi imao pristup relevantnim informacijama i kako bi obavljao svoje radne zadatke. Svako računalo može imati više administratora te više korisnika. Same lozinke ujedno mogu biti i slaba točka zaštite sustava, ali zbog ljudskog faktora.[67]

Sljedeći korak u zaštiti informacijskih sustava je zaštita korisničkih programa. Nakon što pomoću korisničkog imena i lozinke uđemo u sustav tj. radnu površinu, pokreće se program kojim se obavlja određena aktivnost u informacijskom sustavu.

Korisnički programi se štite na način da se pojedinim korisnicima dodaju ovlasti te ako određuju funkcije koje mogu obavljati u programu. Postoje tri razine ovlasti:

- Prva razina – služi isključivo i samo čitanje iz baze podataka
- Druga razina – koristi se prilikom postupka izmjena postojećih podataka u bazi i dodavanje novih podataka
- Treća razina – primjenjuje se za brisanje podataka iz baze

Kako bi se organizacija zaštitila od zlonamjernog korištenja ovlasti radnika postoji još jedan korak povećanju sigurnosti informacijskog sustava.

[66] Čizmić J., Boban M., Zlatović D., *Nove tehnologije, intelektualno vlasništvo i informacijska sigurnost*. Split: Sveučilište u Splitu Pravni fakultet, 2016.;
[67] *Ibidem*;

Naime, svi podaci koji se mijenjaju ili brišu spremaju se u posebne direktorije u sustavu kojima pristup ima samo administrator. Tek kada on odluči da podaci nisu potrebni oni se trajno brišu iz sustava.[68]

#### *5.2.2.1. Organizacija mjera zaštite infomacija*

Organizacijske mjere su one mjere koje poduzima sam poslovni sustav s ciljem osiguranja željene razine funkcionalnosti sustava te integriteta podataka u uvjetima djelovanja pretpostavljenih oblika prijetnji. Organizacijskim mjerama smatra se sveukupni sadržaj mjera i postupaka iz oblasti sigurnosti, izrada potrebne dokumentacije koja je potrebna za njihovu primjenu te donošenje i izrada organizacijskih uputa kojima se one provode na radnom mjestu.[69]

Postoji nekoliko razina informacijske sigurnosti. To su infrastruktura informacijske sigurnosti, sigurnost pristupa treće osobe te *outsourcing*. Svima njima je cilj zaštita informacijskog sustava.[70]

[68] Čizmić J., Boban M., Zlatović D., *Nove tehnologije, intelektualno vlasništvo i informacijska sigurnost*. Split: Sveučilište u Splitu Pravni fakultet, 2016.;
[69] Šehanović, J., Hutinski Ž., Žugaj M., *Informatika za ekonomiste*, Tiskara Varteks, 2002, str.237. ;
[70] *Ibidem*, str. 138. ;

# 6. TAJNOST OSOBNIH PODATAKA U POLICIJSKOM POSTUPKU

Ključni pojmovi vezani uz temu zlouporabe podataka označavaju pojam osobnih podataka, odn. podatke koji se pripisuju određenoj osobi, te pojam privatnosti ili pravo svake osobe na vlastitu privatnost. Prema *Zakonu o zaštiti osobnih podataka,*[71] osobni podaci su definirani kao „svaka informacija koja se odnosi na identificiranu fizičku osobu ili fizičku osobu koju je moguće identificirati; osoba koja se može identificirati je osoba čiji se identitet može utvrditi izravno ili neizravno, posebice na temelju identifikacijskog broja ili jedne ili više karakteristika specifičnih za njezin fizički, psihički, mentalni, ekonomski, kulturni ili društveni identitet."[72]

Iz ovo se razloga ‚osobni podaci mogu definirati kao širok raspon različitih podataka koji mogu izravno i neizravno dovesti do otkrivanja identiteta određene osobe.[73] Svaka zlouporaba osobnih podataka napad je na privatnost osobe jer se njezin identitet može otkriti.

Privatnost je nešto što se često spominje, kao i sintagma „pravo na privatnost" koja se smatra jednim od osnovnih prava svakog čovjeka. „Privatnost je jedna od temeljnih vrijednosti zapadne pravne kulture.

Temelji se, na uvjerenju da svako ljudsko biće ima vrijednost po sebi, a s druge na iskonskoj ljudskoj potrebi za postojanjem određenog zaštićenog prostora iz kojeg bi svi ostali bili psihički i materijalno isključeni.[74]

[71] Internet izvor: https://www.zakon.hr/z/220/Zakon-o-zaštiti-osobnih-podataka (29.7.2022.);
[72] M. Boban, *Sigurnost i zaštita osobnih podataka - pravni i kulturološki aspekti : doktorska disertacija*. Zagreb : Filozofski fakultet u Zagrebu : Odsjek za informacijske znanosti, 2012. Str. 11.;
[73] *Ibidem*;
[74] K. Antoliš, I. Varjačić, M. Jelenski*: Combating Cyber Crime, Academic and Applied Research in Military and Public Management Scienc*e, Year 2018 (HU ISSN 2498-5392) Vol 17, Issue 3, pp19-46, Budimpešta, Hungary;

## 6.1. Internetska zaštita podataka

Fizičke metode zaštite jedna su od ključnih komponenti u cjelokupnoj zaštiti informacijskog sustava. Fizička sigurnost informacijskog sustava ugrožava se u slučajevima elementarnih nepogoda te ljudskih ranjivosti, kao što je sabotaža, krađa i neposlušnost. Primjena fizičke sigurnosti podrazumijeva proces uporabe mjera zaštite kako bi se spriječio neovlašten pristup, oštećenje ili uništenje dobara.[75] Fizička sigurnost smatra se osnovom informacijske sigurnosti te su ostale sigurnosne mjere utemeljene upravo na njoj.[76]

Pravila EU o zaštiti podataka jamče zaštitu vaših osobnih podataka svaki put kada se prikupljaju, na primjer kada kupite nešto na internetu, prijavite se na natječaj za posao ili podnesete zahtjev za bankovni kredit. Primjenjuju se i na tvrtke i organizacije (javne i privatne) u EU-u i one sa sjedištem izvan EU-a, ali pružaju robu ili usluge u EU-u, kao što su Facebook i Amazon, kad god te tvrtke traže ili ponovno koriste osobne podatke pojedinaca u EU-u.

Nije važno u kojem su formatu podaci. Bilo u elektroničkom ili papirnatom obliku, kad god se pohranjuju ili obrađuju podaci u kojima se možete izravno ili neizravno identificirati kao pojedinac, vaša prava na zaštitu podataka moraju se poštivati.[77]

Pravila o zaštiti podataka EU-a konsolidirana u Općoj uredbi EU-a o zaštiti podataka (ili CRPD-u) opisuju različite situacije u kojima tvrtke i organizacije mogu prikupljati ili ponovno koristiti vaše osobne podatke:[78]

1 kada s vama sklope ugovor, na primjer o isporuci robe ili usluge (tj. kada nešto kupite putem interneta) ili ugovor o radu
2 kada ispune zakonsku obvezu, na primjer u slučajevima kada je obrada vaših podataka zakonski potrebna, na primjer kada vaš poslodavac daje podatke o vašoj mjesečnoj plaći tijelu socijalnog osiguranja kako biste ostvarili svoje pravo na socijalnu sigurnost
3 kada vam je obrada podataka od vitalnog interesa, na primjer kada vam može spasiti život

[75] Internet izvor: http://www.cert.hr/sites/default/files/NCERT-PUBDOC-2010-06-304.pdf (10.5.2022.);
[76] Klasić, K., Klarin, K., *Informacijski sustavi : načela i praksa*.: Intus informatika, Zagreb 2009., str. 114. ;
[77] Internet izvor: https://europa.eu/youreurope/citizens/consumers/internet-telecoms/data-protection-online-privacy/index_hr.htm (29,7.2022.);
[78] *Ibidem*;

4 u ispunjavanju poslova od javnog interesa, što se uglavnom odnosi na poslove javne uprave kao što su škole, bolnice i općine
5 kada postoje legitimni interesi – na primjer, vaša banka koristi vaše osobne podatke kako bi provjerila imate li pravo na štedni račun s višom kamatnom stopom.

U svim drugim situacijama, tvrtka ili organizacija moraju tražiti vaš pristanak (poznat kao "pristanak") prije nego što mogu prikupiti ili ponovno upotrijebiti vaše osobne podatke.

Kada tvrtka ili organizacija zatraži vaš pristanak, morate joj dati jasnu potvrdnu radnju, kao što je potpisivanje obrasca za pristanak ili odabir odgovora da između jasno ponuđenih odgovora da i ne na web stranici

Nije dovoljno lako odabrati nešto što vas ne zanima, kao što je označiti okvir gdje ne želite primati marketinške e-poruke. Morate aktivno potvrditi i složiti se da će vaši osobni podaci biti pohranjeni i/ili ponovno korišteni u tu svrhu.

Prije nego se odlučite složiti, trebali biste dobiti sljedeće informacije:

1 podatke o tvrtki ili organizaciji koja će obraditi vaše podatke, uključujući njihove podatke za kontakt i kontakt podatke službenika za zaštitu podataka ako ih ima
2 zašto će tvrtka ili organizacija koristiti vaše osobne podatke
3 koliko dugo će čuvati vaše osobne podatke
4 informacije o bilo kojoj drugoj tvrtki ili bilo kojoj drugoj organizaciji koja će primiti vaše osobne podatke
5 informacije o vašim pravima na zaštitu podataka (pristup, ispravak, brisanje, prigovor, povlačenje privole).

Sve ove informacije trebaju biti prikazane jasno i razumno.

### 6.1.1. Postupanje s osobnim podatcima

#### *6.1.1.1. Pristup*

Pristup osobnim podacima koje određena tvrtka ili organizacija ima o pojedincima se može zatražiti. Također, isti imaju pravo dobiti kopiju osobnih podataka u dostupnom formatu i besplatno. Organizacija treba odgovoriti u roku od mjesec dana i dati kopiju osobnih podataka i relevantne informacije o tome kako su informacije korištene ili se koriste.[79]

#### *6.1.1.2. Ispravljanje i prenošenje*

Ukoliko tvrtka ili organizacija pohranjuje osobne podatke (o osobama) koji sadrže netočnosti ili su nepotpuni, može se zatražiti ispravljanje ili ažuriranje podataka.

#### *6.1.1.3. Brisanje*

U određenim situacijama se od tvrtke ili organizacije može zatražiti ovraćanja podataka ili izravan prijenos istih drugoj tvrtki ukoliko je to tehnički izvedivo. To je poznato kao "prenosivost podataka". Npr., ovo pravo se može koristiti ukoliko se želite prebaciti s jedne usluge na drugu sličnu uslugu, kao što je jedna društvena mreža na drugu, i želite da se vaši osobni podaci brzo i jednostavno prenesu na novu uslugu.

Ako osobni podaci više nisu potrebni ili se koriste nezakonito, može se zatražiti njihovo brisanje, što se zove "pravo na zaborav".

[79] K. Antoliš, I. Varjačić, M. Jelenski: *Combating Cyber Crime, Academic and Applied Research in Military and Public Management Science, Y*ear 2018 (HU ISSN 2498-5392) Vol 17, Issue 3, pp19-46, Budimpešta, Hungary;

Ova pravila vrijede i za tražilice, poput Googlea, jer se i one smatraju vodećima u obradi podataka. Možete zatražiti da se veze na web stranice koje sadrže vaše ime uklone iz rezultata pretraživanja ako su informacije netočne, neprikladne, irelevantne ili pretjerane.

Ako je tvrtka učinila vaše osobne podatke dostupnima na internetu i zatražite njihovo brisanje, tvrtka mora obavijestiti sve druge web stranice s kojima se podaci dijele da ste zatražili brisanje podataka i poveznica na njih.

Neki podaci se možda neće automatski izbrisati radi zaštite drugih prava kao što je sloboda izražavanja. Na primjer, kontroverzne izjave ljudi koji su u centru pažnje ne mogu se izbrisati ako je u javnom interesu ostati online.

## 6.2. Neovlašten pristup osobnim podatcima

Ako su osobni podaci ukradeni, izgubljeni ili im se pristupilo nezakonito, ili je došlo do "povređivanja osobnih podataka", voditelj obrade podataka (osoba ili tijelo koje obrađuje vaše osobne podatke) mora to prijaviti nacionalnom tijelu za zaštitu podataka. mora obavijestiti vlasnika podataka izravno ako postoje ozbiljni rizici za vaše osobne podatke ili privatnost zbog te povrede.

Ako se smatra da prava na zaštitu podataka nisu poštovana, postoji mogućnopst podizanja tužbe izravno nacionalnom tijelu za zaštitu podataka, koje će ispitati pritužbu i odgovoriti u roku od tri mjeseca. Umjesto da prvo kontaktirate nacionalno tijelo za zaštitu podataka, možete pokrenuti pravni postupak protiv tvrtke ili organizacije izravno na sudu.

Ako ste pretrpjeli materijalnu (kao što je financijski gubitak) ili nematerijalnu štetu (kao što je psihička patnja) jer tvrtka ili organizacija ne poštuje pravila o zaštiti podataka EU-a, možda imate pravo na naknadu.[80]

[80] Internet izvor: https://europa.eu/youreurope/citizens/consumers/internet-telecoms/data-protection-online-privacy/index_hr.htm (29.7.2022.);

# 7. ZAKLJUČAK

Jedan od najbitnijih uslova za sigurnost, općenito, u društvu i osobnu sigurnost građana kao i za sigurnost poslovanja predstavlja informacijsko-komunikacijska sigurnost. U pitanju je funkcioniranje svih struktura države i društva koja je važna za sigurnost svakog građana, dok se s druge strane radi o ostvarivanju slobode i prava građana i njihovom statusu u društvu, te položaju prema državnoj i poslovnoj strukturi.

Osnova za ostvarivanje informacijske sigurnosti se nalazi u međunarodnim i nacionalnim propisima. Bitno je da su informacije u službi čovjeka, osobne slobode, sigurnosti i napredovanja kao i to da ostvarivanje informacijske sigurnosti znači stvaranje uvjeta sigurnosti čovjeka i građna.

Povijesni razvoj međunarodne policijske suradnje obilježen je geopolitičkim i gospodarskim promjenama u rasponu od tradicionalnih oblika međunarodne policijske suradnje do očuvanja autokratskog političkog režima kroz uspješnu i učinkovitu međunarodnu policijsku suradnju danas kroz bilateralnu i uglavnom regionalnu suradnju. policijsku suradnju.

Informacijska sigurnost je postupak, koji ukazuje da se neprekidno razvijaju novi sustavi zaštite informacijskog sustava. Razlog tome je neprekidan razvoj novih alata koji mogu ugroziti sigurnost informacijskog sustava poput „zloćudnog“ softwarea (virusi), koji prilikom upada u informacijski sustav mogu napraviti veliku štetu, poput krađe podataka, koji mogu dovesti i do krađe novčanih sredstava sa bankovnih računa. Također se razvijaju i novi načini poslovne špijunaže, koja ne mora biti samo računalne prirode.

Pristupanje informacijsko-komunikacijskoj sigurnosti u Republici Hrvatskoj, kao i izgradnja sustava informacijske sigurnosti se usklađuje s pristupom i standardima Europske Unije kao i NATO-a, pa se tako, u skladu s navedenim daje početna definicija prema kojoj sustav informacijske sigurnosti obuhvaća ljude, postupke, organizacije, tehnologiju.

# 8. LITERATURA


- Antoliš K., Varjačić I., Jelenski M.*: Combating Cyber Crime, Academic and Applied Research in Military and Public Management Scienc*e, Year 2018 (HU ISSN 2498-5392) Vol 17, Issue 3, pp19-46, Budimpešta, Hungary;
- Boban M, Perišić M., *Biometrija, Zbornik radova Veleučilišta u Šibeniku*, No.1-2/2015, srpanj 2015, str. 115-148.;
- Boban M., *Sigurnost i zaštita osobnih podataka - pravni i kulturološki aspekti : doktorska disertacija*. Zagreb : Filozofski fakultet u Zagrebu : Odsjek za informacijske znanosti, 2012. Str. 11.;
- Čerić, V., Varga, M., 2004., *Informacijska tehnologija u poslovanju*, Sveučilište u Zagrebu, Element, Zagreb;
- Čizmić J., Boban M., Zlatović D., *Nove tehnologije, intelektualno vlasništvo i informacijska sigurnost*. Split: Sveučilište u Splitu Pravni fakultet, 2016.;
- Dimitrijević, Vojin (1973.) *Pojam sigurnosti u međunarodnim odnosima*. Beograd: Savremena administracija;
- https://europa.eu/youreurope/citizens/consumers/internet-telecoms/data-protection-online-privacy/index_hr.htm (29.7.2022.);
- https://www.zakon.hr/z/220/Zakon-o-zaštiti-osobnih-podataka (29.7.2022.);
- *Informacijska sigurnost, zaštita podataka, osobnih podataka i informacija* http://www.cert.hr/sites/default/files/NCERT-PUBDOC-2010-06-304.pdf (28.7.2022.);
- Klaić A., Perešin A.: *Zbornik radova*; Dani kriznog upravljanja 2011. 678-708 str. Veleučilište Velika Gorica 2011.
- Klasić, K., Klarin, K., *Informacijski sustavi : načela i praksa*.: Intus informatika, Zagreb 2009., str. 114. ;
- Kostanjevec A. i dr.. *Sigurnost informacijskih sustava verzija* 01012014, FOI Varaždin 2014. str.2.;
- Luić Lj.: *Informacijski sustavi*, Veleučilište u Karlovcu, Karlovac 2009; str.36.;

- Miletić, Andreja (1978.) *Nacionalni interes u američkoj teoriji međunarodnih odnosa*. Sarajevo - Beograd: Savremena administracija;
- POLICIJSKI ETIČKI KODEKS ZA POLICIJSKE SLUŽBENIKE UPRAVE POLICIJE MINISTARSTVA UNUTRAŠNJIH POSLOVA KANTONA SARAJEVO, dostupno na: https://mup.ks.gov.ba/sites/mup.ks.gov.ba/files/policijski_eticki_kodeks.pdf (22.7.2022.);
- Rhodes-Ousley M., *Information Security*: *The Complete Reference, Second Edition, McGraw Hill Professional*, 2013.;
- Schwartz, P.M., „*The Computer in German and America Constitutional Law: Towards an American Right of Information Self-Determination*, American Journal of Comparative Law, 1989., vol. 37;
- Stouffer K., Lightman S., Pillitteri V., Abrams M., Hahn A., *Guide to Industrial Control Systems (ICS) Security, NIST- National Institute of Standards and Technology*, Gaithersburg, Svibanj 2014., str. 156.;
- Strenburner, G., Goguen, A., Feringa, A., *Risk Management Guide for Infromation Tehnology System*, NIS – National Institute of Standard and Tehnology, U.S. Department of Commerce, July 2002.
- Šehanović, J., Hutinski Ž., Žugaj M., *Informatika za ekonomiste*, Tiskara Varteks, 2002, str.237.;
- Tatalovic S., Bilandzic M., (2011.), *Osnove nacionalne sigurnosti* str. 23.;
- *Zakon o policijskim službenicima Kantona Sarajevo* („Službene novine Kantona Sarajevo“ broj: 38/18)
- Zakon o zaštiti osobnih podataka Republike Hrvatske, dostupno na: https://www.zakon.hr/z/220/Zakon-o-zaštiti-osobnih-podataka (19.7.2022.);
- *Zakon o zaštiti osobnih podataka*, („Službeni glasnik Bosne i Hercegovine“, broj 49/06, 76/11 i 89/11), dostupno na: https://fzs.ba/wp-content/uploads/2016/06/zakon_podaci.pdf (25.7.2022.);

# 9. SAŽETAK

***Zaštita tajnosti podataka – regulativni okvir i procedure u postupanju policijskih službenika***

Informacijska sigurnost je postupak, koji ukazuje da se neprekidno razvijaju novi sustavi zaštite informacijskog sustava. Razlog tome je neprekidan razvoj novih alata koji mogu ugroziti sigurnost informacijskog sustava poput „zlućudnog“ softwarea (virusi), koji prilikom upada u informacijski sustav mogu napraviti veliku štetu, poput krađe podataka, koji mogu dovesti i do krađe novčanih sredstava sa bankovnih računa. Također se razvijaju i novi načini poslovne špijunaže, koja ne mora biti samo računalne prirode. Kroz ovaj se rad prikazuje pojam informacijske sigurnosti, kroz obradu teme koja je vezana za pojmove zaštite sigurnosti osobnih podataka u policijskom postupanju.

**Ključne riječi**: sigurnost, informacijska sigurnost, policija, tajnost podataka, osobni podatci

## *10. ABSTRACT*

***Data confidentiality protection - regulatory framework and procedures in the conduct of police officers***

*Information security is a process that indicates that new information system protection systems are constantly being developed. The reason for this is the continuous development of new tools that can threaten the security of the information system, such as "malicious" software (viruses), which when breaking into the information system can cause great damage, such as data theft, which can also lead to the theft of funds from bank accounts. New ways of business espionage are also being developed, which does not have to be computer-based only. Through this paper, the concept of information security is presented, through the processing of a topic related to the concepts of personal data security protection in police procedures.*

***Keywords**: security, information security, police, data confidentiality, personal data*

# 11. ŽIVOTOPIS

**Ime i prezime**: Slaven Šutalo

**Datum i mjesto rođena** :24.04.1984. godine u Čapljini, BiH

**Adresa stanovanja:** Tekera 99, općina Ljubuški

**Obrazovanje:**

1991./1999 godine Osnovna škola Ivane Brlić Mažuranić-Humac, općina Ljubuški

1999./2003. godine Gimnazija Ljubuški

2007./2008. godine Policijska akademija Sarajveo

2010./2013. godine CEPS Kiseljak , smjer Cestovni promet, gdje stječem zvanje prvostupnika cestovnog prometa

**Radno iskustvo:**

2008. godine zasnivam radni odnos kao policijski službenik MUP-a ŽZH raspoređen na radno mjesto u Postrojbi za sigurnost cestovnog prometa –prometnik

2017./2022. godine raspoređen na radno mjesto Voditelja smjene u PU Grude

2022. godine raspoređen na radno mjesto Pomoćnika zapovjednika za promet PU Grude

**Publikacije (autor) :**

-Vukoja Mate, Žulja Goran,Kružić Ivana,Jerković Ivan, Anđelinović Šimun,Šimić Stipe, Marendić Slobodan, Šutalo Slaven, Bašić Željana, Jasak Tomislav et al.

Forenzična analiza tragova krvi,Split:Slobodna Dalmacija,2021 (monografija)

**Ostalo:**

Po zasnivanju radnog odnosa u MUP-u ŽZH osim navedenog školovanja pohađao sam veći broj seminara,tečajeva,stručnih usavršavanja i konferencija koje su bile organizirane na području

FBiH i RH a koje su,u suradnji sa MUP-om ŽZH bile organizirane od strane vladinih i nevladinih organizacija te pojedinih stručnjaka iz raznih oblasti. Od navedenih aktivnosti posebno bi izdvojio aktivno sudjelovanje u PSP programu u organizaciji PH International BiH u suradnji Vlade SAD-a koja ujedno i financira cijeli projekt a čiji temelji leže na dijelu programa FBI-a –odjel narkotika. U sklopu navedenog u Sarajevu sam 2021. godine završio andragošku obuku te stekao zvanje PSP trenera. Od 2014. godine također sam i aktivni član međunarodnog policijskog udruženja IPA te sam kroz proteklo razdoblje sudjelovao na brojnim aktivnostima koje su se održavale na području Europe. U slobodno vrijeme posvećen sam obitelji i svoje dvoje djece te sviranju glazbenih instrumenata (harmonika, gitara, klavijatura) .

# 12. IZJAVA O AKADEMSKOJ ČESTITOSTI

SVEUČILIŠTE U SPLITU
Sveučilišni odijel za forenzične znanosti

*Izjava o akademskoj čestitosti*

Ja Slaven Šutalo , izjavljujem da je moj diplomski rad(zaokružite odgovarajuće) pod naslovom Zaštita tajnosti podataka – regulativni okvir i procedure u postupanju policijskih službenika rezultat mojeg vlastitog rada, da se temelji na mojim istraživanjima, da se oslanja na izvore i radove navedene u bilješkama i popisu literature. Nijedan dio ovog rada nije napisan na nedopušten način, odnosno nije prepisan bez citiranja i ne krši ičija autorska prava. Izjavljujem da ni jedan dio ovog rada nije iskorišten u ijednom drugom radu pri bilo kojoj drugoj višeškolskoj, znanstvenoj, obrazovnoj ustanovi. Sadržaj mojeg rada u potpunosti odgovara sadržaju obranjenoga i nakon obrane uređenoga rada.

Split, kolovoz, 2022. godine

Potpis studenta: _____
Slaven Šutalo