Informacijska sigurnost i zaštita podataka u policijskim postupcima

Jasak, Tomislav

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:227:173679

SVEUČILIŠTE U SPLITU

SVEUČILIŠNI ODIJEL ZA FORENZIČNE ZNANOSTI

ISTRAŽIVANJE MJESTA DOGAĐAJA

DIPLOMSKI RAD

INFORMACIJSKA SIGURNOST I ZAŠTITA PODATAKA U POLICIJSKIM POSTUPCIMA

TOMISLAV JASAK

Split, lipanj, 2022.

SVEUČILIŠTE U SPLITU

SVEUČILIŠNI ODIJEL ZA FORENZIČNE ZNANOSTI

ISTRAŽIVANJE MJESTA DOGAĐAJA

DIPLOMSKI RAD

INFORMACIJSKA SIGURNOST I ZAŠTITA PODATAKA U POLICIJSKIM POSTUPCIMA

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

TOMISLAV JASAK

503/2019

Split, lipanj, 2022.

Rad je izrađen u: Grude, Bosna i Hercegovina

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

u vremenskom razdoblju od 12.5.2022. do 11.6.2022. godine

Datum predaje diplomskog rada: 15. lipanj 2022.

Datum prihvaćanja rada: 20. lipanj 2022.

Datum usmenog polaganja: 27. lipanj 2022.

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

2. Doc. dr. sc. Marina Carić

3. Izv. prof. dr. sc. Marija Boban

SADRŽAJ

1. UVOD 1

2. CILJ RADA 2

2.1. Hipoteze 2

2.2. Struktura rada 3

3. INFORMACIJSKA SIGURNOST 4

3.1. Pojam sigurnosti 4

3.1.1. Prijetnje sigurnosti 5

3.2. Suvremene tehnologije – informacijska sigurnost 8

3.2.1. Informacijski prostor 8

3.3. Informacijski sustav – sigurnost i prijetnje (ratovanje) 9

3.4. Informacijski sustav – zaštita i sigurnost podataka 11

3.4.1. Procjena rizika 12

3.5. Policijska djelatnost – razvoj suvremene tehnologije i zaštita privatnosti 13

3.5.1. Kibernetičke prijetnje i napadi 14

3.6. Zaštita informacijskog sustava i podataka 17

3.6.1. Fizičke mjere zaštite 17

3.6.2. Programske mjere zaštite 17

3.6.3. Organizacijske mjere zaštite 19

4. PRIVATNOST I SIGURNOST OSOBNIH PODATAKA 20

4.1. Zaštita privatnih podataka na internetu 20

4.2. Provala i pristup podatcima 22

4.3. Pristup osobnim podatcima 22

4.4. Ispravak i prenošenje osobnih podataka 23

4.5. Perijenos osobnih podataka (brisanje/zaborav) 23
4.6. Neovlašten pristup vašim podatcima 24
4.7. Pritužbe 24
4.8. „Kolačići“ prilikom pretraživanja 24
5. INFORMACIJSKA SIGURNOST I ZAŠTITA PODATAKA U POLICIJSKIM POSTUPCIMA – PRIMJER ČEDOMORSTVA 26
5.1. Zakonske odredbe – kazneno značenje djela 29
5.2. Postojanje kaznenog djela 31
5.3. Forenzična analiza čedomorstva 32
5.3.1. Obdukcija 32
5.3.2. Vanjski pregled žrtve 33
5.3.3. Unutarnji pregled žrtve 34
6. ISTRAŽIVANJE 35
6.1. Primjer 35
6.2. Osvrt na istraživanje 38
7. MEĐUNARODNA POLICIJSKA SURADNJA 39
7.1. Trenutno stanje – razvoj međunarodne policijske suradnje 41
8. ZAKLJUČAK 44
9. LITERATURA 46
10. SAŽETAK 49
11. ABSTRACT 50
12. ŽIVOTOPIS 51
13. IZJAVA O AKADEMSKOJ ČESTITOSTI 53

1. UVOD

„Kriminal nema granice“, izjava je koja zvuči kao klišej, ali zapravo najbolje izražava opseg kriminalne aktivnosti. Osobe uključene u kriminalne radnje ne poznaju granice, zakone, političku, vjersku ili rasnu pripadnost, ne poznaju procedure, ne zamaraju se pravilima i zaštitom državnog suvereniteta i prava. Kriminal funkcionira bez ikakvih ograničenja i pravila. I premda svijest o potrebi suradnje između institucija za provedbu zakona raste iz dana u dan, opći je dojam da su ljudi uključeni u kriminalne radnje uvijek korak ispred institucija. Najveći razlog tome su kompliciranе procedure pregovaranja i postizanja sporazuma o međunarodnoj suradnji na bilateralnoj ili multilateralnoj razini, koja se nakon postizanja sporazuma mora uobličiti u jedan od akata s pravnom snagom.

Takvi propisi se mogu primjenjivati samo nakon dugotrajnih i jasno propisanih postupaka. Stoga mogu proći godine od uočavanja i osvještavanja novog oblika kriminaliteta, preko pronalaženja načina za njegovo rješavanje, oblikovanja načina rješavanja, usklađivanja radnji i zakonskih odredbi, izglasavanja i/ili potvrđivanja dogovorenog rješenja, pružanja svih instrumente za provedbu. u nekim slučajevima desetljećima. Postupci i dogovori osoba koje se bave kriminalnim radnjama, u njihovom jedinom zajedničkom cilju stjecanja nematerijalne ili materijalne koristi, svode se na kratak dogovor o podjeli imovine i možda stisak ruke.

Uspjehu kriminalnih aktivnosti doprinosi brza razmjena informacija putem suvremenih oblika komunikacije, poput interneta i mobitela, brzog i učinkovitog prijevoza robe i osoba te slobodnog kretanja ljudi, te političkih nesuglasica među državama.

Isključivo povezana akcija u obliku organiziranih i koordiniranih mjera svih država može dijelom spriječiti ili usporiti djelovanje pojedinaca ili kriminalnih skupina, a u tu svrhu prvenstveno treba jačati međunarodnu policijsku suradnju.

2. CILJ RADA

S obzirom na to da je sigurnost i zaštita podataka jedna od najvažnijih uvjeta koji se moraju poštivati tijekom obavljanja policijskih dužnosti i policijskih postupaka, kroz ovaj rad će se naglasiti pojam zaštite i stanja sigurnosti podataka u policijskim postupcima. Glavni cilj pisanja ovog rada se ogleda u analizi stanja sigurnosti i zaštite podataka u policijskim postupcima, odnosno za vrijeme postupanja policijskih službenika. S ciljem kvalitetnije obrade teme, kroz rad će se navesti primjer infanticida. Primjerom se želi navesti način djelovanja policijskih službenika, te odnos prema sigurnosti i zaštiti podataka osoba koje su u slučaju od početka do okončanja istog.

2.1. Hipoteze

Informacijska sigurnost, kao i zaštita podataka u policijskim postupanjima se ogleda u tajnosti komunikacija između policijskih službenika s jedne i počinitelja kaznenih djela s druge strane. Informacijska sigurnost i zaštita podataka čine temelj policijske djelatnosti i uspjeha njihovog djelovanja na određenim slučajevima. Uslučaju kršenja etičkih normi od strane policijskih službenika, odnosno u slučajevima „curenja“ informacija, postoji mogućnost stvaranja situacije u kojoj dolazi do otežavanja policijskih posupanja, točnije do otežavanja okončanja određenog slučaja na kojem se radi. Kažnjavanje kršenja pravila poštivanja informacijske sigurnosti, privatnih i podataka o slučaju koji je u tijeku, vremenom se mora postrožiti, s ciljem da bi se uputilo na ozbiljnost značenja pojma privatnih informacija i zaštite podataka od strane, kako policijskih službenika, a tako i druge strane koja sudjeluje u policijskim postupcima.

2.2. Struktura rada

Ovaj rad se sastoji od nekoliko dijelova koji ga zajedno čine jedinstvenom cjelinom, te upućuju na glavnu temu i problematiku koja je za istu vezana. Prvi dio rada govori o pojmovima koji su usko vezani za temu. Ovaj se dio proširuje općenitim uvođenjem u značenje teme rada, te se nadovezuje na glavni dio rada.

Drugi dio, odnosno glavni dio rada sadrži razradu teme, koja se ogleda u tumačenju primjera, analiziranju i komentiranju istih, te uspoređivanju stanja vezanih za primjere koji su navedeni u radu.

Treći dio rada sadrži zaključke teme, ovo je ujedno posljednji dio rada.Ovdje se nalaze osvrti i komentari na prethodno napisane i iznesene analize, kao i primjere na kojima se temelje provedena analiziranja. Zaključni dio sadrži i osobne osvrte na pojmove vezane za temu rada, kao i komentare, te prijedloge koji su osobne prirode i vezani su za mišljenje u prvom licu jednine.

Cilj pisanja ovog rada se ogleda u naglašavanju važnosti očuvanja informacijske sigurnosti i zaštite podataka prilikom postupanja policijskih službenika. Cilj je i analizirati, te komentirati stanja koja se navode kroz rad tako da se pokušava pronaći idealno rješenje za postojeće probleme informacijske sigurnosti i zaštite podataka u djelovanju policijskih službenika.

Svi podatci i informacije uvrštene u rad se oslanjaju na postojeću literaturu koja se navodi na kraju rada. Literatura korištena prilikom pisanja ovog rada je temeljena na prijedlozima mentora.

3. INFORMACIJSKA SIGURNOST

U ovom će se poglavlju, pored pojma sigurnosti, prikazati pojmovi povijesnog tijeka razvoja informacijske sigurnosti, kao i pojmovi sigurnosnih podataka, te rizične točke informacijske sigurnosti.[1]

3.1. Pojam sigurnosti

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.[2]

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 da li je 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.[3]

Možemo objasniti četiri temeljna, odnosno osnovna pristupa proučavanja pojma sigurnosti. Tako da imamo četiri vrste sigurnosti:[4]

[1] 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;
[2] Čizmić J., Boban M., Zlatović D., *Nove tehnologije, intelektualno vlasništvo i informacijska sigurnost*. Split: Sveučilište u Splitu Pravni fakultet, 2016.;
[3] Tatalovic S., Bilandzic M., (2011.), *Osnove nacionalne sigurnosti* str. 23.;
[4] Dimitrijević, Vojin (1973.) *Pojam sigurnosti u međunarodnim odnosima*. Beograd: Savremena administracija;

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
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.[5]

3.1.1. Prijetnje sigurnosti

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.[6]

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[7]:

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

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
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:[8]

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

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;
5 Uređuje procedure i način organizacije službe vezano za kretanje i boravak stranaca u Bosni i Hercegovini;
6 forenzička ispitivanja i vještačenja.

U sklopu ovog ministarstva (Bosne i Hercegovine), 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.[9]

[9] *Ibidem*;

3.2. Suvremene tehnologije – informacijska sigurnost

3.2.1. 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.[10]

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 posljednjih nekoliko desetljeća mogu se utvrditi neke karakteristične faze kroz koje je oblikovanje javnog informacijskog prostora prolazilo.[11]

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.[12]

---

[10] Rhodes-Ousley M., *Information Security*: *The Complete Reference, Second Edition, McGraw Hill Professional*, 2013.;
[11] Klaić A., Perešin A.: *Zbornik radova*; Dani kriznog upravljanja 2011. 678-708 str. Veleučilište Velika Gorica 2011.
[12] Čizmić J., Boban M., Zlatović D., *Nove tehnologije, intelektualno vlasništvo i informacijska sigurnost*. Split: Sveučilište u Splitu Pravni fakultet, 2016.;

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.[13]

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.[14]

3.3. Informacijski sustav – sigurnost i prijetnje (ratovanje)

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.[15]

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:[16]

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

[13] Luić Lj.: *Informacijski sustavi*, Veleučilište u Karlovcu, Karlovac 2009; str.36.;
[14] Šehanović J. i dr.: *Informatika za ekonomiste*, Sveučilište u Rijeci, Pula 2002., str. 50.;
[15] Čizmić J., Boban M., Zlatović D., *Nove tehnologije, intelektualno vlasništvo i informacijska sigurnost*. Split: Sveučilište u Splitu Pravni fakultet, 2016.;
[16] *Zakon o informacijskoj sigurnosti*, NN 79/07;

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.[17]

Pored zakona informacijska sigurnost definirana je i ISO 27001 standardom:[18] 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:[19]

1 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;[20]
2 sigurnosni incident – naznačen jednim ili nizom neželjenih ili neočekivanih sigurnosnih događaja koji imaju značajnu vjerojatnost ugrožavanja poslovnih aktivnosti i informacijske sigurnosti;
3 zaštita – nositelja svih informacija potrebnih za nesmetan rad poslovnog sustava. Zaštita podrazumijeva provođenje mjera poradi osiguranja informacijskog sustava;
4 ranjivost – s obzirom na to da je sustav ranjiv, pa tako postoji rizik da informacija bude izložena neovlaštenom pristupu. ISO 27002 ranjivost definira kao:[21] „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.[22]
5 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. (Sustav upravljanja uključuje organizacijsku strukturu, politike, planiranje aktivnosti, odgovornosti, vježbe, procedure, procese i resurse.) Rizik je u literaturi opisan kao funkcija razine prijetnje, ranjivosti i vrijednosti informacijske

[17] Kostanjevec A. i dr.. *Sigurnost informacijskih sustava verzija* 01012014, FOI Varaždin 2014. str.2.;
[18] *Ibidem*;
[19] *Ibidem*;
[20] Čizmić J., Boban M., Zlatović D., *Nove tehnologije, intelektualno vlasništvo i informacijska sigurnost*. Split: Sveučilište u Splitu Pravni fakultet, 2016.;
[21] Boban M, Perišić M., *Biometrija, Zbornik radova Veleučilišta u Šibeniku,* No.1-2/2015, srpanj 2015, str. 115-148.;
[22] *Ibidem*;

imovine. izik se jasnije može opisati kao vjerojatnost prijetnje da iskoristi neku ranjivost imovine te time ugrozi imovinu.[23]

3.4. Informacijski sustav – zaštita i sigurnost 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 primjenom informacijske komunikacijske tehnologije (eng. *Information and Communication Technology* – ICT).

Cilj IS-a 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.[24]

Bitno je naglasiti i temeljne aktivnosti poslovnog sustava:[25]

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

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

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.[26]

3.4.1. 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.[27]

Sigurnosni rizik se definira kao mogućnost realizacije nekog neželjenog događaja. Neželjeni događaj može utjecati na:[28]

- 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

[26] *Ibidem*;
[27] 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.
[28] *Ibidem*;

tehnologije i alata itd. Bez adekvatno provedene analize ranjivosti, skoro je nemoguće odrediti sigurnosni rizik. [29]

3.5. Policijska djelatnost – razvoj suvremene tehnologije i zaštita privatnosti

Kibernetička sigurnost postaje sve aktuelnija tema u IT [30] i OT [31] sektorima. Uvođenjem interneta u većinu sustava i uređaja (tzv. *Internet of Things*, skraćeno IOT) postaju ICT[32] sustavi sve napredniji i zastupljeniji. Napretkom informacijskih i komunikacijskih tehnologija i ostvarivanjem veza između IT i OT računalnih mreža, te korištenjem komercijalnih PC [33] tehnologija u OT svijetu je dovelo do ugroze do tada sigurnih OT sustava.

Putem interneta odnosno IOT, moguća su dva načina komunikacije u IT i OT sustavima:

** Uređaj – čovjek * Uređaj – 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.

[29] *Ibidem*;
[30] *Information Technology* – informacijska tehnologija;
[31] Telekomunikacijski*;
[32] *Information and Communication Technology* – informacijska i komunikacijska tehnologija ;
[33] Kompjuterskih;

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.

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.

3.5.1. Kibernetičke prijetnje i napadi

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 sljedeće:[34]

I. *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.

II. *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.

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

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

V. *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.

VI. *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[35] 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.

VII. *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.

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

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

I. *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 raznih

[35] 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;

državnih i nedržavnih institucija samo jednim klikom sa računala koje se ni ne nalazi u blizini mete.[36]

II. *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

III. *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.[37]

IV. *Kibernetički rat* – rat koji se vodi uz pomoć računala i računalnih mreža. Najčešće je barem jedan od sudionika države. 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 kibernetički terorizam, kibernetičku špijunaži i kibernetički kriminal u svrhu napada na protivnika.[38]

[36] 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.;
[37] Čizmić J., Boban M., Zlatović D., *Nove tehnologije, intelektualno vlasništvo i informacijska sigurnost*. Split: Sveučilište u Splitu Pravni fakultet, 2016.;
[38] 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.;

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

3.6. Zaštita informacijskog sustava i podataka

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.

3.6.1. 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.[39] Fizička sigurnost smatra se osnovom informacijske sigurnosti te su ostale sigurnosne mjere utemeljene upravo na njoj.[40]

3.6.2. Programske mjere zaštite

[39] http://www.cert.hr/sites/default/files/NCERT-PUBDOC-2010-06-304.pdf ;
[40] Klasić, K., Klarin, K., *Informacijski sustavi : načela i praksa*.: Intus informatika, Zagreb 2009., str. 114. ;

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.[41]

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.[42]

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:

1 Prva razina – služi isključivo i samo čitanje iz baze podataka
2 Druga razina – koristi se prilikom postupka izmjena postojećih podataka u bazi i dodavanje novih podataka
3 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.

[41] Čizmić J., Boban M., Zlatović D., *Nove tehnologije, intelektualno vlasništvo i informacijska sigurnost*. Split: Sveučilište u Splitu Pravni fakultet, 2016.;
[42] *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.[43]

3.6.3. Organizacijske mjere zaštite

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.[44]

Postoji nekoliko razina informacijske sigurnosti. To su infrastruktura informacijske sigurnosti, sigurnost pristupa treće osobe te *outsourcing*. Svima njima je cilj zaštita informacijskog sustava.[45]

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

4. PRIVATNOST I SIGURNOST OSOBNIH PODATAKA

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,*[46] 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."[47]

Stoga se osobni podaci mogu definirati kao širok raspon različitih podataka koji mogu izravno i neizravno dovesti do otkrivanja identiteta određene osobe.[48] 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.[49]

4.1. Zaštita privatnih podataka na internetu

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,

[46] Internet izvor: https://www.zakon.hr/z/220/Zakon-o-zaštiti-osobnih-podataka (10.5.2022.);
[47] 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.;
[48] *Ibidem*;
[49] 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;

oštećenje ili uništenje dobara.[50] Fizička sigurnost smatra se osnovom informacijske sigurnosti te su ostale sigurnosne mjere utemeljene upravo na njoj.[51]

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.[52]

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:[53]

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
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.

[50] Internet izvor: http://www.cert.hr/sites/default/files/NCERT-PUBDOC-2010-06-304.pdf (10.5.2022.);
[51] Klasić, K., Klarin, K., *Informacijski sustavi : načela i praksa*.: Intus informatika, Zagreb 2009., str. 114. ;
[52] Internet izvor: https://europa.eu/youreurope/citizens/consumers/internet-telecoms/data-protection-online-privacy/index_hr.htm (11.5.2022.);
[53] *Ibidem*;

4.2. Provala i pristup podatcima

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.

4.3. Pristup osobnim podatcima

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.[54]

[54] 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;

4.4. Ispravak i prenošenje osobnih podataka

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

4.5. Perijenos osobnih podataka (brisanje/zaborav)

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".

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.

4.6. Neovlašten pristup vašim podatcima

Ako su vaši 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 vas obavijestiti izravno ako postoje ozbiljni rizici za vaše osobne podatke ili privatnost zbog te povrede.

4.7. Pritužbe

Ukoliko smatrate da vaša prava na zaštitu podataka nisu poštovana, možete podnijeti pritužbu izravno nacionalnom tijelu za zaštitu podataka, koje će ispitati vašu pritužbu i odgovoriti vam 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.[55]

4.8. „Kolačići“ prilikom pretraživanja

Kolačići predstavljaju male tekstualne datoteke koje web stranica pohranjuje na vaše računalo ili mobilni uređaj putem vašeg internet preglednika. Kolačići se koriste posvuda za pohranjivanje vaših preferencija kako bi web stranice radile učinkovitije. Također se koriste za praćenje vaše upotrebe interneta i izradu korisničkih profila, a zatim za prikaz prilagođenih online oglasa na temelju vaših preferencija.

[55] Internet izvor: https://europa.eu/youreurope/citizens/consumers/internet-telecoms/data-protection-online-privacy/index_hr.htm (11.5.2022.);

Svaka web stranica koja želi koristiti kolačiće mora dobiti vaš pristanak prije postavljanja kolačića na vaše računalo ili mobilni uređaj. Ne bi vas trebali samo informirati o korištenju kolačića ili vam objasniti kako ih možete isključiti.

Web stranica bi vam trebala objasniti kako će se koristiti podaci kolačića. Trebali biste moći povući svoj pristanak. Ako to odlučite, web-mjesto vam i dalje mora pružati najmanju moguću uslugu, kao što je pristup dijelu stranice.

Pristanak nije potreban za sve kolačiće. Nije potreban pristanak za kolačiće koji se koriste isključivo u svrhu prijenosa poruke. To uključuje, na primjer, kolačiće koji se koriste za "ravnotežu opterećenja" (tj. dopuštaju dijeljenje zahtjeva na poslužitelju na više od jednog uređaja). Pristanak također nije potreban za kolačiće koji su nužni za pružanje usluge koju ste izričito zatražili. uključuje, na primjer, kolačiće koji se koriste kada ispunjavate online obrazac ili kada koristite košaricu za kupnju na mreži.[56]

[56] *Ibidem*;

5. INFORMACIJSKA SIGURNOST I ZAŠTITA PODATAKA U POLICIJSKIM POSTUPCIMA – PRIMJER ČEDOMORSTVA

Pojam čedomorstva se objašnjava kao ubojstvo novorođenčeta svjesnom voljom i aktivnostima majke. Gledano kroz povijest, ubijanje novorođenčadi u različitim fazama je imalo različite tretmane. U nekim je društvima bilo dopušteno, dok je u drugima zabranjeno i praćeno najstrožim kaznama. Najveći broj čedomorstava se dogodio u društvima u kojima je majci prijetila smrtna kazna zbog izvanbračnog djeteta. Tek u dvadesetom stoljeću, točnije 1920-ih, odnos prema čedomorstvu je pravno liberaliziran, pa se to čedomorstvo danas tretira kao privilegirano ubojstvo.

Privilegija se ogleda u tome što se poremećaj unaprijed prepoznaje, a ne dokazuje, već pretpostavlja neku zakonsku pretpostavku. Istina je, ako se medicinski promatra, da postoji mali broj određenih izvjesnih poremećaja psihičkog stanja porodilje, ali to nije razlog za uvođenje privilegije.

Čedomorstvo se pojavljuje u kulturno zaostalim sredinama s teškim socijalnim položajem porodilje, ili pak u sredinama koje imaju izuzetno krute moralne stavove. To je jedan od razloga za izdvajanje ovog djela iz opće kaznene politike prema ubojstvu stavljajući ga pod blagu kaznu.

Do ubojstva djeteta pri porođaju može doći na dva načina i to: posljedično (majka priprema krivično djelo, skrivajući trudnoću tijekom njenog trajanja), i situativno (majka se na ubojstvo djeteta odlučuje pod utjecajem posebnog psihofizičkog stanja u vrijeme porođaja) čedomorstvo kao pojam koji podrazumijeva ubijanje tek rođenog djeteta od strane majke poznat je od davnina. čedomorstvo dolazi od dviju rijedi: dedo i umorstvo. Taj naziv ima svoje korijene u latinskoj riječi infaticidium, složenici od riječi infas (dijete) i occido (ubiti).

Riječ "infaticidium" nije primjerena onome Sto u sudsko - medicinskoj terminologiji treba označavati. Postoji stručni naziv koji označava kritičko razdoblje života u kojem se ubojstvo događa, a to je neonatus ili novorođenče. Ali s obzirom na to da je riječ novorođenče presložena za dvosloženicu, koristi se naziv čedo koje mu je sinonim. Tako je kazneno djelo ubojstva novorođenčeta nakon poroda dobilo naziv čedomorstvo.

Iznenadna smrt zdravog tek rođenog djeteta zahtijeva forenzičku i pravnu istragu, a ukoliko forenzička istraga ne uspije otkriti značajan uzrok smrti, dojenče se vodi pod dijagnozom SIDS-a. Od svih diferencijalnih dijagnoza, ubojstvo se rijetko kad smatra mogućim uzrokom smrti, ali su ranije provedena istraživanja pokazala kako je 20% SIDS-a zapravo ubojstvo od strane majke.

Također, treba u vidu imati mogućnost ubojstva, kako bi se zadovoljila pravda djeteta i osigurala buduća zaštita djece. Znanstvenici su ispitali 3 čimbenika koji ograničavaju prepoznavanje ubojstva dojenčeta svrstavajući smrt pod dijagnozu SIDS-a; Prvi čimbenik je zadovoljenje određenih smjernica i protokola za dijagnozu SIDS-a, zatim je ispitana vjerodostojnost pravilno izvedenih obdukcija, kao i utjecaj vlasti i zakona.

Ako se u jednoj obitelji dogodi više od dvije iznenadne smrti dojenčadi, postoji osnovana sumnja za ubojstvo, pored toga da se nužno moraju analizirati sve prethodne smrti. U prilog mogućeg namjernog gušenja govore nalazi rekurentne cijanoze, apneje, ALTE-a koje se događaju u prisutnosti samo jednog od roditelja ili bližnjih srodnika djeteta; podaci o prijašnjim smrtima u obitelji, istovremena smrt blizanaca, podaci o prethodnom krvarenju u plućima.

U ovom slučaju kaznenog djela se radi o privilegiranom djelu delicta propria, koje može izvršiti samo biološka majka djeteta usmrćenjem djeteta, pod uvjetima koje propisuje zakon. Ovaj konstitutivni element ovog kaznenog djela, čini temelj njegove privilegiranosti. Konstitutivni elementi bića kaznenog djela čedomorstva su:

1. počinitelj kaznenog djela može biti samo biološka majka usmrćenog novorođenčeta
2. objekt radnje – kaznenog djela je novorođenče
3. radnja počinjenja kaznenog djela može biti svaka radnja, djelkovanjem ili propuštanjem, koje se smatra uzrokom smrti novorođenčeta
4. posljedica izvršenja kaznenog djela je nastupanje smrti djeteta
5. vrijeme izvršenja kaznenog djela čedomorstva može biti isključivo za vrijeme ili neposredno nakon poroda

Kazneni zakoni ne određuju uvijek točno vrijeme trajanja poremećaja, pa se slučajevi promatraju individualno. Smatra se da se u navedenom vremenskom razdoblju uslijed porođajnih

bolova, porodilja nalazi u izuzetnom fizičkom i psihičkom stanju iz kojeg se javlja poremećaj koji smanjuje njezinu ubrojivost. Taj se poremećaj kod porodilje ne pretpostavlja, nego se utvrđuje u svakom slučaju.

Treba utvrditi njegovu vrstu, narav, intenzitet i vrijeme trajanja kao i utjecaj takvog poremećaja na ponašanje čedomorke tempore criminis, tj. izjasniti se o pitanju njezine uračunljivosti, prisutne za vrijeme počinjenja kaznenog djela.

U sudsko psihijatrijskom pogledu na čedomorstvo se ne može otkriti ili pronaći tvrdnja, opis ili postavka da normalan fiziološki porođaj dovodi do takvih psihičkih poremećaja koji bi direktno ili po analogiji mogli biti svrstani u neku od poznatih ili priznatih kliničkih, tj. psihopatoloških kategorija; iz čega proizlazi činjenica kako psihijatrija ne priznaje ženi porodilji, pri normalnom tijeku događaja prilikom poroda, nikakav poseban psihički status.

Ono što postoji, i u čemu se svi slažu, jest porođajna psihoza, o kojoj je pisano u nastavku rada. Način na koji se saznaje za kazneno djelo čedomorstva je najčešći:

1 prijavom zdravstvenih ustanova,
2 javnim oglašavanjem,
3 putem anonimnih prijava,
4 pronalaskom beživotnog tijela novorođenčeta,
5 samoprijavljivanjem majke,
6 operativnim radom, i dr.

Vrlo je važno da se pored svih dokaza, kako materijalnih tako i osobnih koji se prikupljaju, dobije i priznanje majke, tj. da se saslušanjem osumnjičene svi dokazi poklope i da se logički povežu. Dakle kod kaznenog djela ubojstva djeteta pri porođaju, počinitelj može da bude, kao što je već ranije navedeno, samo majka, u kriminalističkoj obradi je potrebno da sudjeluju žene policijski službenici.

U slučajevima kada je za čedomorstvo osumnjičena majka koja je maloljetna, istragu treba da vodi policijski službenik za maloljetnike.

Tragovi koji ukazuju na porođaj su sljedeći: pri porođaju djeteta iz maternice se izlijeva plodna voda, boja plodne vode je sivožuta do žutozelenkasta. Mikroskopski je lako dokazivo

postojanje tih mrlja, mrlje dječje pogani su slične mrljama trave ili tamno zelenkaste sluzi , koža novorođenčeta je djelomično pokrivena sirastom sluzi.

Navedeni tragovi se mogu naći na različitijim predmetima kojima je novorođenče došlo u dodir ili na kojima se odvijao porođaj. Tragovi navedenog porođaja se mogu utvrđivati i liječničkim pregledom majke.

5.1. Zakonske odredbe – kazneno značenje djela

U Kaznenom zakonu, glava deseta, Kaznena djela protiv života i tijela, Članak 112. – Usmrćenje, stavka (2) glasi: Majka koja usmrti svoje dijete pod utjecajem jakog duševnog opterećenja zbog trudnoće ili poroda kaznit će se kaznom zatvora od šest mjeseci do pet godina.Djelo mora biti počinjeno pod utjecajem jakog duševnog opterećenja zbog trudnoće ili poroda. Prema Krivičnom zakonu obilježje bića kaznenog djela bio je poremećaj koje kod majke izazvao porod i bilo je potrebno utvrditi da je majka usmrtila svoje dijete upravo zbog tog poremećaja.

U KZ/97 je izostavljen poremećaj kao obilježje bića kaznenog djela što je dovelo do rasprave oko toga je li tu okolnost i nadalje potrebno utvrđivati u postupku ili se ona presumira. Slabost takvog tumačenja je u neosnovanom privilegiranju majke čije ponašanje nije uvjetovano psihopatološki niti socijalno i koja na temelju prethodno stvorene odluke hladnokrvno i iz egoističkih pobuda lišava života svoje dijete tijekom poroda ili neposredno nakon njega.

Vrhovni sud je zaključio da nakon što je Kazneni zakon izmijenjen, više nije potrebno utvrđivanje postojanja poremećaja što kod počiniteljice ovog dijela izaziva porod, već je djelo ostvareno kada majka usmrti svoje dijete za vrijeme ili nakon poroda.

Poremećaj se nepresumira niti je unaprijed isključeno, već je njegovo postojanje potrebno utvrditi u svakom konkretnom slučaju. Jako duševno opterećenje zbog trudnoće ili poroda obuhvaća poremećaj, ali je ujedno i šire od tog pojma.

Osim poremećajem, duševno opterećenje može biti uvjetovano i socijalnim razlozima. Ono može proizlaziti iz teškog socijalnog položaja majke ili iz toga što bi je sredina odbacila zbog

izvanbračnog djeteta ili što je izložena obiteljskom nasilju ili se nalazi u stanju izrazito teške depresije izazvane porodom.U sudskoj praksi se i dosad vrlo restriktivno tumačila odredba o tome do kojeg se vremena može raditi o čedomorstvu, a nakon kojega se radi o teškom ubojstvu. Tako majka koja je svoje dijete usmrtila bacivši ga u more devetnaesti dan po izlasku iz bolnice ne odgovara za čedomorstvo već za teško ubojstvo.

Premda, prema shvaćanju suda, postoji teoretska mogućnost da poremećaj izazvan porodom traje i 21 dan nakon poroda, za optuženu koja je lišila života svoje dijete pet dana po porodu ne može se smatrati da je počinila kazneno djelo pod utjecajem tog poremećaja. Naša novija sudska praksa prihvaća 24 sata od poroda kao gornju granicu nakon koje se više ne radi o čedomorstvu već o teškom ubojstvu.

S obzirom na to da jako duševno opterećenje može biti zazvano ne samo porodom već i trudnoćom proizlazi da se o čedomorstvu kao privilegiranom usmrćenju radi i ako je majka odluku da ubije dijete donijela za vrijeme trudnoće. To stoga što je već i stanje trudnoće, a ne samo poroda, prema novom zakonskom rješenju prikladno prouzročiti jako duševno opterećenje trudne žene. Bez obzira na drugačije zakonsko uređenje, i u dosadašnjoj je sudskoj praksi bilo dominantno shvaćanje da se isključuje pravnu kvalifikaciju čedomorstva okolnost da je trudna žena donijela odluku o usmrćenju djeteta prije nego što je porod započeo. Novo hrvatsko kazneno zakonodavstvo, to jest kazneno zakonodavstvo nakon prvih višestranačkih izbora znatno se razlikuje od onoga u prijašnjem razdoblju.

Stupnjevanjem ljudskih života prema vrijednosti osobe, a što uključuje i vrednovanje prema starosti žrtve, strano je kaznenom pravu. Osim toga KZ/97 upao je u proturječnost jer je istu okolnost, ubojstvo djeteta, u članku 91. tretirao kao kvalifikatornu, a u članku 93. kao privilegirajuću. To znači da je ubojstvo djeteta izravno nakon poroda privilegirano, a ono koje je počinjeno nakon toga kvalificirano, iako je navedenu vremensku razliku teško podvući i praksa je u tom pogledu neujednačena. Osim toga, Zakon nije bio dosljedan jer ako je uzrast žrtve učinio kvalifikatornom okolnošću kod ubojstva, morao je to učiniti i kod tjelesnih ozljeda, a možda i u nizu drugih kaznenih djela. Moderni zakonici ne predviđaju ubojstvo djeteta i maloljetnika kao kvalificirano, s iznimkom francuskog Kaznenog zakona.

Brisana je točka 2. KZ/97, jer je nelogično da stjecaj dvaju običnih ubojstava ne predstavlja teško ubojstvo pa je kažnjava blaže nego stjecaj ubojstva jedne osobe i njezina ploda, kojemu Kazneni zakon pruža manju zaštitu nego čovjeku nakon rođenja.

5.2. Postojanje kaznenog djela

Tri osnovna standarda koja se moraju zadovoljiti po kaznenom zakonu za kriminalno djelo su: namjera, motiv i prilika. Poštivajući tri standarda, majka je primarni osumnjičenik jer provodi najviše vremena s dojenčetom, a namjera ubojstva, najčešće ugušenjem, zahtijeva minimalno planiranje i sredstvo ubojstva joj je često na dohvat ruke. Takav mehanizam ugušenja korištenjem jastuka ili ruke ostavlja manjkav ili nikakav forenzički dokaz.[57]

Kao motiv čedomorstav se najčešće navodi siromaštvo, nezrelost i nespremnost na majčinstvo ili stres kojeg predstavlja dojenče koje neprekidno plače te služi kao okidač za ubojstvo.

Konkretan, točan broj ubojstava nije poznat zbog više razloga: ubojstvo ugušenjem se ne može razlučiti od SIDS-a na patološkoj razini, nedostatak detaljne forenzičke istrage, ubojice se ponašaju kao žrtve i društvo ih simpatizira i negira kao ubojice, SIDS je prihvatljivo objašnjenje za sve okolnosti.

Histološki pregled plućnog tkiva može otkriti uzrok nasilne smrti s izvedenom toksikološkom analizom na lijekove, otrove i predoziranja.

[57]Gluščić, S., *Pregled međunarodne policijske suradnje u okviru Europske unije*, Policija i sigurnost, Zagreb, godina 21., 2012. godine, broj 1;

5.3. Forenzična analiza čedomorstva

Detaljna analiza mjesta iznenadne smrti novorođenčeta je itekako bitna iz razloga jer nosi oko 90% konačne dijagnoze i otkrivanja uzroka smrti. Vjeruje se kako pažljivo prikupljanje podataka povećava dijagnostičku točnost i preciznost rezultata, standardizirani pristup istraživanju te kategorizira uzroke smrti čime poboljšava preventivne strategije. U svrhu otkrivanja kaznenog djela čedomorstva je formirana velika radna multidisciplinarna skupina (SUIDIRF) kojoj je glavni zadatak razvoj i osmišljavanje smjernica koje su izdane pod nazivom *Sudden Unexplained Infant Death Investigation Investigative Top 25.* [58]

U sklopu zadataka i prikuopljanja informacija koje doprinose okončanju postupka istrage je nabrojano je 25 najčešćih čimbenika na koje treba obratiti pažnju tijekom postupka istraživanja uzroka iznenadne dojenačke smrti.

Čimbenici uključuju detaljnu anamnezu, znakove asfiksije, podatke o dijeljenju kreveta s roditeljima, poremećaje prilikom spavanja, hipertermiju ili hipotermiju, čimbenike okoline kao što je ugljični monoksid, kemikalije, prehrana, podaci o nedavnim hospitalizacijama dojenčeta, prethodne kliničke dijagnoze, povijest o ALTE-u, povijest o zdravstvenoj njezi bez postavljene dijagnoze, podaci o nedavnim povredama ili padovima, povijest o korištenju lijekova i otrova, potencijalni prirodni uzroci, podaci o prethodnim susretima s policijom ili socijalnom službom, podaci o smrti rođaka, zahtjevi za donaciju organa ili tkiva, objektivnost provedene obdukcije, mjere reanimacije, svaka sumnjiva okolnost, detaljan opis okolnosti koje bi dovele do smrti.

5.3.1. Obdukcija

Postupak obdukcije podrazumijeva vanjski i unutarnji sistematski pregled, pregled lubanje, prikupljanje tkiva za mikroskopsku analizu, prikupljanje uzoraka krvi i likvora, toksikološki probir

[58] Deflem M., *International Policing in Nineteenth-Century Europe: The Police Union of German States*, 1851-1866, International Criminal Justice Rewiew, 1996, str. 36.

kao i probir na urođene poremećaje metabolizma.[59] Trebao bi se primjeniti i pratiti, također i razgovor s neuropatologom i pedijatrom kardiologom. Uzimajući u obzir financijsko stanje u zdravstvu, probir za procjenu srčanog ritma kao i strukturne anomalije bi trebao postati rutinski postupak u vođenju obdukcije.

U sklopu postupka obdukcije kao forenzičke analize u postupku okončanja i dolaska do saznanja o samom slučaju, poznajemo vanjski i unutarnji pregled žrtve, o čemu je pisano u nastavku.[60]

5.3.2. Vanjski pregled žrtve

Vanjski pregled se sastoji od detaljne analize svih vanjskih površina tijela žrtve. Prisustvo krvnih podljeva – hematoma, kožnih vezikula ili pustula, petehije, uvučene fontanele, mrtvačke pjege na neuobičajenim mjestima na tijelu trebaju usmjeravati na dijagnozu s poznatim uzrokom smrti, a ne na SIDS.

Moguća je vizualizacija retine direktnom ili indirektnom oftalmoskopijom s ciljem da se prikažu eventualna krvarenja. Prikupljaju se uzorci krvi, likvora i nazofaringealni bris za uvid u mogućnost postojanja infektivnog uzročnika nastanka smrti.

Po završetku postupka vanjskog pregleda se izvodi radiološko snimanje kostura - skeleta tzv. *babygram*, gdje važnu ulogu imaju kraniogram, radiogram grudnih organa, abdomena, zdjelice, ekstremiteta, s posebnim radiogramima za šake i stopala u lateralnoj i antero-posteriornoj projekciji.[61]

[59] Huang P., Rongjun Y., Shiying L. ,Zhiqiang Q., Ningguo L., Jianhua Z., i sur. (2013.) *Sudden twin infant death on the same day*;
[60] *Ibidem*;
[61] *Ibidem*;

5.3.3. Unutarnji pregled žrtve

Unutarnji pregled se sastoji od postupaka detaljne analize svakog pojedinog organa kod žrtve. Broj dijagnostičkih, nespecifičnih nalaza koji se često nalaze prilikom obdukcije dojenčeta koje je umrlo iznenadnom smrću je velik, ali se moraju interpretirati u kontekstu cjelovite istrage i okolnosti smrti.

Takvi nalazi podrazumijevaju kongestiju, edem ili krvarenje u plućima, petehije na timusu, epikardu i visceralnoj pleuri te manja, fokalna krvarenja u mozgu.

Prilikom pregleda srca je moguće otkriti zaživotno postojanje urođenih anomalija koje su dovele do smrti novorođenčeta. Poredd analiziranja pojedinih organa se uzima i uzorak tkiva i tekućina za provođenje toksikoloških analiza, metaboličkog probira, serologiju, genetička istraživanja i histološki pregled.[62]

Nakon detaljne analize mjesta smrti, mikroskopija ima jedan od najvećih doprinosa u utkrivanju uzroka iznenadne dojenačke smrti, iz razloga što otkriva uzročnike infektivnih procesa, metaboličkih poremećaja (npr. manjak MCA-CoA dehidrogenaze kod masno promijenjene jetre), kardiomiopatija (npr. histiocitoza, endokardijalna fibrozna stenoza) ili neoplazmi (npr. endokardijalni rabdomiom).[63]

Napredovanjem tehnologije mogućnost sekvencioniranja cijelog genoma može otkriti točan uzrok smrti novorođenčadi umrlih od SIDS-a.[64]

[62]Andrew T., (2016.),*The continuing enigma of sudden infant unexpected death*;
[63] Walsh, J.K., Farrell, M.K., Keenan, W.J., Lucas, M., & Kramer, M. (1981). *Gastroesophageal reflux in infants: relation to apnea.* The Journal of Pediatrics, 99, 197–201.;
[64] Shekhawat, P.S., Matern, D., Strauss, A.W. (2005). *Fetal fatty acid oxidation disorders, their effect on maternal health and neonatal outcome: impact of expanded newborn screening on their diagnosis and management*. Pediatric Research, 57, 78R–86R.;

6. ISTRAŽIVANJE

U ovom djelu diplomskog rada smo izvršili osvrt da dosadašnja istraživanja kaznenog djela čedomorstva na teritoriju Bosne i Hercegovine, točnije na prostoru Županije Zapadno-hercegovačke.

Kroz poglavlje smo uvrstili prikaz slučaja infanticida, odnosno čedomorstva, te smo (preko predočenih fotografija) izvršili prikaz rezultata istraživanja, tj. postupka vođenja slučaja. Na početku poglavlja smo izvršili komentar samog kaznenog djela, dok se drugi dio ovog poglavlja bazira na fotografijama prikupljene dokumentacije vezane za vođenje postupka istrage i forenzičkih aktivnosti, do same presude. Prikupljena dokumentacija je dio stvarnog događaja koji je počinjen 2018. godine. Više podataka i detalja je prikazano u nastavku poglavlja.

6.1. Primjer

Primjer iz prakse: Čedomorstvo 169 KZ F BIH: Majka koja usmrti svoje dijete za vrijeme ili izravno nakon poroda kaznit će se kaznom zatvora od jedne do 5 godina.

Prva saznanja i sačinjavanje bilješke na okolnosti operativnih saznanja: Službena bilješka sačinjena na temelju članka 234. ZKP FBiH dana 10.09.2018. godine, u prostorijama PU Grude, od strane policijskog službenika OKP-a PU Grude, a na okolnosti prikupljenih operativnih saznanja- informacija da se među građanima zaseoka Dragićina, priča o nestanku novorođenog djeteta obitelji, odnosno da isti ne pričaju niti želi pričati sa susjedima na temu gdje je dijete, odnosno isti izbjegava bilo kakvu komunikaciju po pitanju navedene situacije i samog statusa djeteta.

Dana 09.09.2018. godine došao sam do saznanja od uporišta na terenu da je dana 01.09.2018. godine, subota na porodiljinom odjelu SKB Mostar, obitelj dobila četvrto dijete, neprovjereno se radi o ženskom djetetu, koje je porodio dr. Grizelj, i koje je nakon samog poroda bilo živo i zdravo, te je pokazano članovima obitelji. Kako je supruga kroz priču građana mjesta Dragićina cijelo

vrijeme prikrivala trudnoću i negirajući istu kada je dolazilo do upita susjeda i rodbine, je davalo dodatnu sumnju na cjelokupno stanje, jer se navodno dijete ne nalazi u obitelji, a supružnici ne otkrivaju gdje se isto nalazi ili što se dogodilo da isto nije sa svojom obitelji. Po neprovjerenim saznanjima supruga je u srijedu, dana 05.09.2018. godine, otpuštena iz bolnice, te je ista kući došla bez djeteta, te o trenutnom stanju istog ne želi govoriti.

Dana 11.09.2018. godine, upućen je poziv u svojstvu svjedoka suprugu za dan 12.09.2018. godine u 09.00 sati, s kojim će se obaviti obavijesni razgovor i koji će se saslušati o trenutnom statusu djeteta, i cjelokupne situacije, te će se tijekom saslušanja po prikupljenim podrobnijim saznanjima upoznati i pozvati Centar za socijalni rad Grude, radi eventualnog postupanja iz svoje nadležnosti, gdje će se o saslušanju prethodno usmeno upoznati ravnatelj navedenog centra. Postupajući po navedenim informacijama dana 12.09.2018. godine za koje smo saslušanje izvršili određene pripreme, (točnije smo se detaljnije pripremili za isto jer smo smatrali da će otac biti zatvoreniji i da neće htjeti odgovarati na naša pitanja), u službene prostorije je pristupio otac, koji je prilikom obavljanja obavijesnog razgovora policijskim službenicima kroz razgovor priznao da je dana 06.09.2018. godine oko 16.30 sati na dijelu regionalne ceste R-424 Mostar - Čitluk, odložio svoje tek rođeno dijete, kojom prilikom se s navedenim u vozilu nalazila njegova supruga i dvoje malodobne djece, te su po povratku svojoj obiteljskoj kući, prikrili razlog ne dovođenja djeteta kući.

Isti je pristao policijske službenike odvesti na mjesto gdje je dijete ostavljeno. O unaprijed navedenom je upoznata dežurna tužiteljica ŽT ŽZH Široki Brijeg, PU Mostar, Sektor kriminalističke policije ŽZH-a MUP-a HNŽ-a, koji su na mjestu pronalaska tijela u prisutnosti dežurnog tužitelja izvršili očevidne radnje, točnije tijelo nije pronađeno na mjestu na koje je isti ukazao gdje ga je odložio, nego je isto pronađeno odbačeno oko 50 metara u provaliji, te je isto prevezeno u Gradsku mrtvačnicu Bijeli Brijeg, gdje će se nad tijelom izvršiti obdukcija, s ciljem utvrđivanja nastanka smrti.

Prema uputama postupajućeg tužitelja u 12.40 sati otac je predan službenicima sektora kriminalističke policije MUP-a HNŽ na daljnje postupanje, zato što se djelo dogodilo na području kojeg pokriva njihova PU, dok je u prostorijama PU Grude u svojstvu svjedoka odmah pozvana i saslušana majka, a ista je saslušanja u svojstvu svjedoka, zato što se u prvom djelu nisu odmah utvrdile sve činjenice i prikupili dokazi, a posebno što se po porodu (40 dana) ista nalazila u stanju

postporođajne depresije, zbog čega se konkretnije postupanje vezano za istu čekalo, odnosno da bude zdravstveno sposoban, i da bi se mogla utvrđivati njena odgovornost (iako su mediji zbog tih stvari prozivali institucije za nepostupanje prema istoj).

Odmah po upoznavaju sa situacijom je upoznat Centar za socijalni rad, koji je po službenoj dužnosti donio rješenje, o izuzimanju djece i njihovu smještanju na skrb i brigu u majčino selo Međugorje. Od majke je na potvrdu o privremeno oduzetim predmetima sukladno čl.80 ZKP-a FBiH (dragovoljna predaja), izuzet mobilni uređaj majke, koji će se naknadno vještačiti s ciljem pronalaska dokaza koji se mogu dovesti u vezu s navedenim događajem.

Navedeno djelo je po utvrđivanju činjenica i izvršene obdukcije prekvalificiramo u Ubojstvo čl.166 KZ F BiH. Na prijedlog Kantonalnog tužiteljstva Mostar, Kantonalni sud Mostar je izdao Naredbu, za izuzimanje neposrednih uzoraka – bris bukalne sluznice od majke, koje će izuzeti stručna osoba u prisutnosti ovlaštenih osoba i krim tehničara MUP-a ŽZH-a PU Grude, kako bi se isti na osnovu sljedeće izdate Naredbe mogli usporediti njezin nesporni DNA profil s DNA profilom koji je uzet na obdukciji, a radi utvrđivanja identiteta novorođene bebe.

Isto tako postupajući tužitelj je naložio da se prije postupka suđenja izvrši psihološko vještačenje i procjeni da li je osoba sposobna da sudjeluje u sudskom postupku (radnja poduzeta prije okončanja svih istražnih radnji), dok je psihijatrijsko vještačenje izvršeno tijekom same istrage i podnošenja optužnice. Sukladno uputama postupajućeg tužiteljstva osoba je lišena slobode nakon izvršenog očevid i potvrđivanja navoda prijave, i isti je zadržan i pritvoru do sudske presude, a dok je majka tijekom postupka se nalazila na slobodi, a istoj su bile izrečene određene mjere zabrane. U navedenom predmetu su svjedočili policijski službenici OKP-a, na koji način su došli i do kojih saznanja, te o svim poduzetim mjerama i radnjama sukladno zakonu.

U navedenom predmetu Županijski sud Mostar je donio presudu u trajanju od 15 godina zatvora ocu, dok je majka osuđena na 14 godina zatvora, dok se ostala djeca još nalaze smještena u Majčinom selu Međugorje, dok je skrb o djeci preuzela socijalna radnica iz majčinog sela.

6.2. Osvrt na istraživanje

Čedomorstvo je privilegirano usmrćenje koje čini majka koja usmrti svoje dijete pod utjecajem jakog duševnog opterećenja zbog trudnoće ili poroda. Radi se o posebnom kaznenom djelu koje može počiniti samo majka prema svom djetetu. No neće se svako usmrćenje djeteta od strane majke smatrati privilegiranim već samo ono koje je majka počinila pod utjecajem jakog duševnog opterećenja zbog trudnoće ili poroda.

Upravo je zbog te okolnosti, a ne zbog toga što je djelo počinila majka, čedomorstvo jedno od privilegiranih usmrćenja. Privilegiranost čedomorstva ogleda se u propisanoj kazni koja je lakša od kazne za ubojstvo odnosno teško ubojstvo. Stav zakonodavca u odnosu na ovo kazneno djelo se kroz povijest mijenjao ovisno o moralnim nazorima i razvitku medicinske znanosti.

Kroz čitav srednji vijek čedomorke su osuđivane na smrt s posebno teškim način egzekucije kao zakapanje žive čedomorke, nabijanje na kolac, utapanje. Niti pristup hrvatskog zakonodavca prema ovom kaznenom djelu nije uvijek bio jednak. Kroz povijest nalazimo vrlo stroge kazne, ali u novije vrijeme i iznimno blage. Neki autori s pravom ukazuju na to da kod čedomorstva zakonodavac često ide iz krajnosti u krajnost.

Za razumijevanje i razjašnjavanje kaznenih djela čedomorstva, policijski službenici koji provode kriminalističko istraživanje, pored „temeljnog“ znanja o medicini i taktici razjašnjavanja krvnih delikata, trebaju imati i neka osnovna znanja o trudnoći i porodu. Kod istraživanja kaznenog djela čedomorstva treba znati da je trudnoća stanje ženskog organizma u kojem se razvija plod. Trudnoća može biti pravilna ili patološka, a traje 40 tjedana, odnosno 280 dana računajući od prvog dana posljednje mjesečnice. Trudnoća može biti okončana pobačajem ili porodom koji može biti normalan, kompliciran ili patološki.

Tijekom kriminalističkog istraživanja čedomorstva potrebna je žurnost, ali s prijavljivanjem kaznenog djela ne treba žuriti dok se ne prikupe sva relevantna saznanja, prije svega o uzroku smrti, novorođenosti, živorođenosti i donesenosti djeteta.

7. MEĐUNARODNA POLICIJSKA SURADNJA

Cjelokupna globalizacija, koja je zahvatila sve dijelove društva, a posebno je pomogla i značajno utjecala na širenje aktivnosti osoba uključenih u kriminalne radnje, istaknula je međunarodnu suradnju agencija za provođenje zakona kao jedan od glavnih čimbenika u zajedničkim naporima svih zemalja. . za učinkovito sprječavanje, otkrivanje i borbu protiv novih oblika kriminala.[65]

Razvojem društva razvijao se i kriminal, pa danas „moderni organizirani kriminal ima obilježja marketinško orijentiranih aktivnosti, s tendencijom preuzimanja političke kontrole, nasiljem kao sredstvom za postizanje ciljeva i područjem djelovanja u više zemalja. ."

Činjenica da koncept međunarodne policijske suradnje sadrži međunarodni aspekt otežava ga definiranje. U fokusu ovog rada je operativni dio međunarodne policijske suradnje koji se odnosi na međunarodne potrage, a definicija međunarodne policijske suradnje ograničena je na ovaj aspekt.

S gledišta međunarodne suradnje, međunarodna policijska suradnja definira se kao: „suradnja policijskih tijela različitih država koju ta tijela provode na zahtjev druge države ili međunarodne organizacije, djelujući u skladu s međunarodnom ili nacionalnom policijom. propisi ".[66]

Prostorno, međunarodna policijska suradnja može se ostvariti na globalnoj, regionalnoj i bilateralnoj razini. Izvori prava na takvu policijsku suradnju su međunarodni multilateralni i bilateralni sporazumi te domaće i domaće pravo, koje obuhvaćaju provedbene i organizacijske propise, propise koji uređuju postupanje policijskih tijela i aktivnosti drugih tijela za provedbu zakona.[67]

Od svog institucionalnog početka, međunarodna policijska suradnja uključuje policijske aktivnosti poput razmjene informacija o zločinima i počiniteljima, a nedavno su se intenzivirali i

[65] Pavišić, B., Modly, D. i Veić, P.: *Kriminalistika 1, Knjiga prva*, Treće izmijenjeno i dopunjeno izdanje, Golden marketing – Tehnička knjiga, Zagreb, 2006. godina, str. 195 – 196;
[66] *Ibidem*;
[67] Mujanović, E.: *Međunarodna policijska saradnja*, Fakultet za kriminalistiku, kriminologiju i sigurnosne studije Univerziteta u Sarajevu, 2015., str. 9.

drugi oblici policijske suradnje, poput zajedničkih kriminalističkih istraga u kojima je uključeno više zemalja, prikupljanja dokaza putem nacionalnog nadzora i nadzora. počinitelja kaznenih djela na području druge države, a u iznimnim slučajevima i primjenu mjera prisile kao što je prekogranični progon počinitelja teških kaznenih djela.[68]

Međunarodna policijska suradnja temeljila se na osnovnoj ideji borbe protiv međunarodnog kriminala, uz poštivanje međuovisnosti, pravne osnove, specifičnih nadležnosti, koje su uključivale tri temeljne razine. Prva razina suradnje ostvaruje se donošenjem pravnih normi koje reguliraju međunarodnu policijsku suradnju.

Zakonodavstvo stvoreno na ovoj razini suradnje odnosi se na bilateralne i multilateralne sporazume općeg ili posebnog sadržaja. Ugovori o općim sadržajima uređuju opću suradnju državnih policijskih agencija, koja se sastoji od provedbe mjera i radnji za zajedničko suzbijanje svih kategorija kaznenih djela, dok se sporazumima o posebnim sadržajima uređuje provedba zajedničkih mjera i radnji za suzbijanje pojedinih kategorija kaznenih djela.

Pravna regulativa osnovni je preduvjet za drugu i treću razinu suradnje. Dakle, druga razina suradnje podrazumijeva stvaranje policijskih organizacija i drugih službi i agencija zaduženih za policijsku suradnju kako bi se uspostavili stalni kontakti između više nacionalnih policijskih snaga. Karakteristika ove faze je suradnja kroz izravne kontakte i razmjenu informacija između policijskih službenika zaduženih za kriminalističko istraživanje i unapređenje istražnih tehnika.[69]

Treća razina odnosi se na konkretnu suradnju u sprječavanju i rasvjetljavanju počinjenih kaznenih djela. Suradnja se ostvaruje pružanjem pomoći u konkretnim postupovnim i procesnim radnjama u vezi s kaznenim djelima koja nisu bitna za državu u kojoj se pomoć pruža, na pr. prilikom provjere podataka o svjedocima kaznenih djela i sl.

Ova razina uključuje suradnju u borbi protiv teškog kriminala povezanog s organiziranim kriminalom ili terorizmom. Osnovno načelo na kojem se temelji međunarodna policijska suradnja, a koje su prihvatile sve međunarodne policijske organizacije, je poštivanje nacionalnog suvereniteta svake države članice organizacije. Suradnja će se temeljiti na nacionalnim i međunarodnim propisima koji zabranjuju postupanje u pitanjima političkog, vjerskog, rasnog ili

[68] *Ibidem*;
[69] *Ibidem*;

vojnog podrijetla i zalažu se za jednakost i univerzalnost bez ikakvih ograničenja političke, geostrateške ili jezične prirode.

Iako je općeprihvaćeno da je institucionalna međunarodna policijska suradnja posljedica nedavne globalizacije, političkih i gospodarskih promjena, slobodnog tržišta i kretanja ljudi te novijeg datuma, istina je da korijeni međunarodne policijske suradnje sežu u središte 19. stoljeća.

Naime, već sredinom 19. stoljeća zapadne zemlje počele su modernizirati i profesionalizirati svoja tijela za provođenje zakona, što je osiguralo ne baš stabilan, ali početni temelj za razvoj institucionalne međunarodne policijske suradnje.[70]

7.1. Trenutno stanje – razvoj međunarodne policijske suradnje

ospodarskoj, pravnoj ili policijskoj suradnji je Lisabonski ugovor ili Ugovor iz Lisabona koji je potpisan 20. 13. prosinca 2007. stupio na snagu 1. prosinca 2009. godine.[71]

Ugovor ne prenosi nove dodatne nadležnosti na Uniju, ali mijenja način na koji Unija ostvaruje svoje postojeće ovlasti jačanjem sudjelovanja i zaštite građana. Iako Ugovor službeno ne potvrđuje primat prava Unije nad nacionalnim pravom, podsjeća na važnost ujednačene primjene sudske prakse Suda Europske unije. Sud je postavio kriterije za izravni učinak prava Europske unije u nacionalnom pravnom poretku.

Tako stvoren koncept europskog prava počinje razlikovanjem pravnog poretka Europske unije i međunarodnog prava te nacionalnog pravnog sustava država članica. Lisabonski ugovor dao je Europskoj uniji mogućnost potpisivanja međunarodnih sporazuma i pridruživanja međunarodnim organizacijama.

Nadležnost Unije je isključiva jer samo ona može donositi pravne akte, dok države članice mogu provoditi samo zakone Europske unije. Nadalje, nadležnost je podijeljena u dijelu u kojem

[70] Krapac, D.: *Međunarodna kaznenopravna pomoć*, Narodne novine d.d., Zagreb, svibanj 2006., str. 21.;
[71] *Pročišćene inačice Ugovora o Europskoj uniji i Ugovora o funkcioniranju Europske unije,* dostupno na: http://www.mvep.hr/hr/hrvatska-i-europska-unija/ugovori/ugovor-iz-lisabona-(prociscena-inacica)/ (15.5.2022.);

države članice mogu donijeti pravno obvezujuće akte ako to Unija nije učinila, a pomaže im se u činjenici da Europska unija donosi mjere za potporu i dopunu politika država članica.

Svojim odlukama Europski sud pravde, kao glavni pokretač razvoja prava Europske unije, stvorio je izravan učinak i nadmoć prava Europske unije na nacionalni pravni poredak i dodijelio pojedincima prava koja proizlaze izravno iz prava Europske unije, bez obzira na pravnih sustava država članica.

Nadmoć europskog prava nad nacionalnim pravom država članica ograničava suverenitet prava država članica, ali i povećava subjektivna prava njihovih građana. U slučaju neslaganja između prava države članice i prava Europske unije, pravo Europske unije uvijek će imati prednost. Ipak, važno je istaknuti da posljedica primjene supremacije prava Europske unije ne znači automatski nevaljanost nacionalnog prava, već primjena načela supremacije pretpostavlja obvezu nacionalnih sudova da primjenjuju pravo Europske unije.[72]

U praktičnom primjeru to znači da sud može donijeti odluku u konkretnom slučaju primjenom prava Europske unije ne čekajući promjenu osporenog pravnog propisa. Ugovorom iz Maastrichta također su postavljeni novi temelji za proširenje međunarodne policijske suradnje, a jedan od prvih značajnijih pomaka je produženje mandata EUROPOL-a od 1. siječnja 2010. EUROPOL postaje agencija Europske unije i njegov se mandat širi na sve oblike teški međunarodni zločin.

Zadaće EUROPOL-a kao agencije odnose se na prikupljanje, pohranu, obradu, analizu i razmjenu informacija i podataka, koji se zatim prosljeđuju nadležnim tijelima za provedbu zakona država članica. Osim što sudjeluje u istragama pružanjem svih relevantnih informacija državama članicama, EUROPOL aktivno potiče nadležna tijela država članica da pokrenu i provode koordinirane istrage te predlaže osnivanje zajedničkih istražnih timova od slučaja do slučaja.

Pruža obavještajnu i analitičku podršku tijekom događaja visoke sigurnosti te priprema procjene prijetnji, strateške analize i izvješća o općoj situaciji. EUROPOL, kao središnja agencija, ima sklopljene operativne sporazume s Australijom, Islandom, Kanadom, Makedonijom, Monakom, Lihtenštajnom, Norveškom, SAD-om, Švicarskom, Albanijom, Srbijom, Kolumbijom, te INTERPOL-om i Eurojustom. EUROPOL je sklopio strateške sporazume s Bosnom i

[72] Mujanović, E.: *Međunarodna policijska saradnja*, Fakultet za kriminalistiku, kriminologiju i sigurnosne studije Univerziteta u Sarajevu, 2015., str. 9.

Hercegovinom, Crnom Gorom, Moldavijom, Rusijom, Turskom, Europskom središnjom bankom, Europskom komisijom, Europskim centrom za praćenje droga i ovisnosti o drogama, OLAF-om, Frontexom, Svjetskom carinskom organizacijom i UN-om. Ured za droge i kriminal.

Trenutačno schengensku pravnu stečevinu u potpunosti provode 22 države članice Europske unije, dok su se četiri države članice pridružile posebnim sporazumima. Irska i Ujedinjeno Kraljevstvo koje je u procesu izlaska iz Europske unije (tzv. Brexit) trenutno djelomično primjenjuju odredbe pravne stečevine, odnosno samo neke njezine dijelove. Osim Hrvatske, u procesu pridruživanja Schengenskom prostoru su Cipar, Bugarska i Rumunjska.

Uspostavom druge generacije Schengenskog informacijskog sustava te boljih i poboljšanih verzija INTERPOL-ovog informacijskog sustava I-24/7, povijest međunarodne policijske suradnje dovedena je do današnjih dana.[73]

[73] Pavišić, B., Modly, D. i Veić, P.: *Kriminalistika 1, Knjiga prva*, Treće izmijenjeno i dopunjeno izdanje, Golden marketing – Tehnička knjiga, Zagreb, 2006. godina, str. 195 – 196;

8. ZAKLJUČAK

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.

Kao rezultat jačanja povjerenja među državama, nije stvoreno područje slobode, sigurnosti i pravde za robe, usluge i slobodno kretanje ljudi, kao ni za bolju, učinkovitiju i učinkovitiju policijsku suradnju u Europi, tj. Europska Unija. Međutim, na drugim kontinentima poput Afrike, Azije i Sjedinjenih Država to povjerenje još nije ojačano, što je rezultiralo zastojem, odnosno nastavkom tradicionalnih, univerzalnih oblika međunarodne policijske suradnje. Ti se oblici, nažalost, stoljećima temelje na načelu međusobne povezanosti i imaju malo ili nimalo povjerenja u pravne sustave drugih zemalja. Isticanjem učinkovite i djelotvorne suradnje policije i prihvaćanjem suradnje kao dužnosti i dužnosti svih zemalja svijeta, moguće je postaviti čvrste temelje za zaštitu vrijednosti čovječanstva i suvremenog društva, odnosno temeljna građanska prava kao što je pravo. prava na život, ljudsko dostojanstvo, slobodu i jednakost.

Informacijska sigurnost predstavlja 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.

Svaki informacijski sustav je dio nekog poslovnog sustava i on je taj koji prikuplja, razvrstava, obrađuje, čuva, oblikuje i raspoređuje podatke po jedinicama poslovnog sustava. Kada se spominje informacijski sustav svi obično pomisle na računala i rad s računalima, ali oni ne moraju biti povezani. Podaci su se obrađivali i prije izuma računala u ručnom dobu obrade podataka. Ta ista metoda se i danas ponegdje koristi.

Informacijski rat predstavlja postupke poduzete kako bi se postigla informacijska superiornost utjecanjem na informacije protivnika, procese temeljene na informacijama, informacijske sustave i računalne mreže dok se u isto vrijeme brane vlastite informacije, postupci temeljeni na informacijama, informacijski sustavi i računalne mreže.

Jedan od najvažnijih ciljeva svake organizacije je osiguranje neprekinutosti, tj. kontinuiteta poslovanja. Danas, kontinuitet poslovanja ovisi od više faktora koji na njega utječu, jedan od tih faktora dakako je informacijska sigurnost tj. zaštita podataka i ostalih resursa u poslovanju. Informacijska sigurnost predstavlja određeni proces, što znači 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 (npr.virusi i sl.) koji mogu prilikom stupanja u informacijski sustav napraviti veliku štetu, kao što su krađe podataka, koji mogu dovesti i do krađe novčanih sredstava sa bankovnih računa. Također, razvijaju se i novi načini poslovne špijunaže, koja ne mora biti samo računalne prirode.

Društvena komponenta medija, isto kao i društveno ponašanje, nije označena tehnologijom, nego tehnologija služi kao oruđe, tj. platforma za prijenos ideja, kulture i sličnih oblika komuniciranja. Ipak, ukoliko u obzir uzmemo argumente pojedinih teoretičara medija, kao što je Baudrillard, tehnologija, odnosno mediji u potpunosti nisu neutralni prema korisnicima, iz razloga što svojom strukturom manje – više usmjerava njegovo ponašanje.

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.

Uvođenje sustava upravljanja sigurnošću informacijskog sustava te implementacija normi iz serije ISO 27000 predstavlja provedbu potrebnih mjera za postizanje zadovoljavajuće razine informacijske sigurnosti unutar organizacije. Tim radnjama i postupcima omogućava nesmetanost obavljanja djelatnosti organizacije, a organizacija postaje prepoznata kao pouzdan i moderan poslovni partner, koja se u svakom trenutku može suočiti s najnovijim sigurnosnim prijetnjama i na vrijeme reagirati na eventualne sigurnosne incidente.

9. LITERATURA

- Andrew T., (2016.),*The continuing enigma of sudden infant unexpected death*;
- 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.;
- Deflem M., *International Policing in Nineteenth-Century Europe: The Police Union of German States*, 1851-1866, International Criminal Justice Rewiew, 1996, str. 36.
- Dimitrijević, V., *Pojam sigurnosti u međunarodnim odnosima*. Beograd: Savremena administracija, 1973.;
- Gluščić, S., *Pregled međunarodne policijske suradnje u okviru Europske unije*, Policija i sigurnost, Zagreb, godina 21., 2012. godine, broj 1;
- Huang P., Rongjun Y., Shiying L. ,Zhiqiang Q., Ningguo L., Jianhua Z., i sur. (2013.) *Sudden twin infant death on the same day*;
- Internet izvor: http://www.cert.hr/sites/default/files/NCERT-PUBDOC-2010-06-304.pdf (10.5.2022.);
- Internet izvor: https://europa.eu/youreurope/citizens/consumers/internet-telecoms/data-protection-online-privacy/index_hr.htm (11.5.2022.);
- Internet izvor: https://www.zakon.hr/z/220/Zakon-o-zaštiti-osobnih-podataka (10.5.2022.);

- 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. ;[1] Kostanjevec A. i dr.. *Sigurnost informacijskih sustava verzija* 01012014, FOI Varaždin 2014. str.2.;
- Krapac, D.: *Međunarodna kaznenopravna pomoć*, Narodne novine d.d., Zagreb, svibanj 2006., str. 21.;
- Luić Lj.: *Informacijski sustavi*, Veleučilište u Karlovcu, Karlovac 2009; str.36.;
- Miletić, A., *Nacionalni interes u američkoj teoriji međunarodnih odnosa*. Sarajevo - Beograd: Savremena administracija, 1987.;
- Mujanović, E.: *Međunarodna policijska saradnja*, Fakultet za kriminalistiku, kriminologiju i sigurnosne studije Univerziteta u Sarajevu, 2015., str. 9.
- Pavišić, B., Modly, D. i Veić, P.: *Kriminalistika 1, Knjiga prva*, Treće izmijenjeno i dopunjeno izdanje, Golden marketing – Tehnička knjiga, Zagreb, 2006. godina, str. 195 – 196;
- *Pročišćene inačice Ugovora o Europskoj uniji i Ugovora o funkcioniranju Europske unije*, dostupno na: http://www.mvep.hr/hr/hrvatska-i-europska-unija/ugovori/ugovor-iz-lisabona-(prociscena-inacica)/ (15.5.2022.);
- 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;
- Shekhawat, P.S., Matern, D., Strauss, A.W. (2005). *Fetal fatty acid oxidation disorders, their effect on maternal health and neonatal outcome: impact of expanded newborn screening on their diagnosis and management*. Pediatric Research, 57, 78R–86R.;
- 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. 155.;

- 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.;
- Walsh, J.K., Farrell, M.K., Keenan, W.J., Lucas, M., & Kramer, M. (1981). *Gastroesophageal reflux in infants: relation to apnea.* The Journal of Pediatrics, 99, 197–201.;
- *Zakon o informacijskoj sigurnosti*, NN 79/07;

10. SAŽETAK

Informacijska sigurnost i zaštita podataka u policijskim postupanjima

Najučinkovitija je razmjena informacija i informacija vezanih uz provedbu potražnih radnji putem međunarodne policijske suradnje. Međunarodna policijska suradnja ostvaruje se razmjenom informacija i informacija između nadležnih policijskih agencija dviju ili više država putem organizacija za međunarodnu policijsku suradnju, koje postupaju na zahtjev druge države u skladu s nacionalnim i međunarodnim pravnim propisima. Ovisno o zakonskom okviru razlikujemo univerzalnu, regionalnu i bilateralnu međunarodnu policijsku suradnju. Policija Republike Hrvatske međunarodnoj policijskoj suradnji pristupa kroz sve oblike međunarodne policijske suradnje i koristi INTERPOL kanal za razmjenu informacija, a putem kanala EUROPOL-a i Schengenskog informacijskog sustava (SIS) kao članica Europske unije. S.I.R. Svrha ovog rada je objasniti aktivnosti istrage, odnosno pokazati sličnosti, razlike, prednosti i nedostatke djelovanja univerzalnih i regionalnih međunarodnih zahtjeva kao jednog od glavnih alata međunarodne policijske suradnje kroz postojeće i korišteni instrumenti potražnje. policijsku suradnju. Uz mnoge sličnosti i razlike, aktivnost pretraživanja i zapljena putem INTERPOL-ovog kanala i schengenskog informacijskog sustava zajednički je cilj, pa nadležna pravosudna tijela kao preduvjet mogu ispuniti svrhu kažnjavanja. za funkcioniranje svake države.

Ključne riječi: informacijska sigurnost, zaštita podataka, policijski službenici, postupanje policije

11. ABSTRACT

Information security and data protection in police proceedings

The most efficient is the exchange of information and information related to the implementation of search operations through international police cooperation. International police co-operation is achieved through the exchange of information and information between the competent police agencies of two or more states through international police co-operation organizations, which act at the request of another state in accordance with national and international legal regulations. . Depending on the legal framework, we distinguish between universal, regional and bilateral international police cooperation. The Police of the Republic of Croatia accesses international police cooperation through all forms of international police cooperation and uses the INTERPOL channel for the exchange of information, and through the EUROPOL channel and the Schengen Information System (SIS) as a member of the European Union. CHEESE. The purpose of this paper is to explain the activities of the investigation, ie to show the similarities, differences, advantages and disadvantages of universal and regional international requirements as one of the main tools of international police cooperation through existing and used demand instruments. police cooperation. With many similarities and differences, the activity of search and seizure through the INTERPOL channel and the Schengen Information System is a common goal, so the competent judicial authorities can fulfill the purpose of punishment as a precondition. for the functioning of each state.

***Keywords**: information security, data protection, police officers, police conduct*

12. ŽIVOTOPIS

88345 Sovići, Grude, Bosna i Hercegovina

Telefon: +387-63-383-888, E-mail: tomislav.jasak@gmail.com mailto:st1pe@hotmail.com

TOMISLAV JASAK

Ime i Prezime: *Tomislav Jasak*
Datum i mjesto rođenja: *29.09.1985 godine u Sarajevu*
Adresa: *Sovići – Podkrstina kbr.240, općina Grude.*

Obrazovanje:

1992/2000 godine osnovnu školu, u školi Fra. Stipana Vrljića – Sovići,

2000/2003 godine završavam srednju trogodišnju, u Obrtničko – industrijskoj Školi Imotski, za zanimanje vozača motornog vozila,

2003/2004 godine završavam četvrtu godinu, u Srednjoj tehničkoj prometnoj školi Split, za zanimanje tehničar cestovnog prometa,

2008/2009 godine završavam policijsku akademiju u Sarajevu,

2012/2015 godine, završavam studij sigurnosti na Visokoj školi „Logos centar“ u Mostaru, na smjeru Kriminalistika gdje stječem zvanje prvostupnika kriminalistike.

Radno iskustvo:

2010- Zasnivam radni odnos kao policijski službenik MUP-a ŽZH, raspoređen na radno mjesto u PU Grude, gdje trenutno radim,

2010 – 2013 – radio sam na temeljnim policijskim poslovima u PU Grude i Ministarstvu unutarnjih poslova Županije Zapadnohercegovačke(pozorno – patrolna djelatnost);

2013 – 2016 – radio sam na poslovima kriminalističkogistražitelja u Odsjek krim. policije u PU Grude;

2016 – 2017 – obavljao sam poslove pomoćnika zapovjednika za promet u PU Grude;

2017 – radim na poslovima Istražitelja kaznenih djela u Odsjeku krim. policije u PU Grude, u činu inspektor.

Publikacije (autor):

- *Vukoja Mate, Žulj Goran, Kružić Ivana, Jerković Ivan, Anđelinović Šimun, Šimić Stipe, Marendić Slobodan, Šutalo Slaven, Bašić, Željana, Jasak Tomislav et al.Forenzička analiza tragova krvi, Split: Slobodna Dalmacija, 2021 (monografija)*

Ostalo:

Po zasnivanja radnog odnosa unutar MUP-a ŽZH, pohađao sam više raznih seminara i tečajeva iz oblasti kriminaliteta i sigurnosti, sudjelovao u raznim konferencijama. Aktivno sudjelujem kao član mjesne zajednice, te se uvijek stavljam na raspolaganje za bilo kakve aktivnosti koje se odnose za najpotrebitije i na najranjiviju skupinu. Svaki slobodni trenutak nastojim provesti uz druženje sa obitelji i prijateljima, otac sam dvoje djece. Dobrovoljni darovatelj krvi sa više puta darivanom krvi, te se rekreativno bavim raznim sportskim aktivnostima.

Tomislav Jasak

13. IZJAVA O AKADEMSKOJ ČESTITOSTI

SVEUČILIŠTE U SPLITU
Sveučilišni odijel za forenzične znanosti

Izjava o akademskoj čestitosti

Ja Tomislav Jasak , izjavljujem da je moj diplomski rad(zaokružite odgovarajuće) pod naslovom Informacijska sigurnost i zaštita podataka u policijskim postupcima 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, lipanj, 2022. godine

Potpis studenta: _____
Tomislav Jasak