VARSTVOSLOVJE,
letn. 19
št. 3
str. 252–272

Integralna korporativna varnost

Miha Dvojmoč

Namen prispevka:

V zadnjih letih je bilo v Sloveniji veliko pozornosti namenjene proučevanju in raziskovanju policijskega dela, policijskih organizacij, zasebnega varovanja in zasebnih varnostnih služb, veliko manj pa integralni korporativni varnosti. Namen prispevka je bralcu prikazati osnove integralne korporativne varnosti in njen obseg.

Metode:

S pomočjo deskriptivne metode in sinteze pridobljenih ter obstoječih znanj smo analizirali in predstavili integralno korporativno varnost. Z analizo vsebine pisnih virov smo naredili pregled domače in tuje literature ter zakonov, ki so pomembni za področje obravnavane tematike.

Ugotovitve:

Po pregledu literature je razvidno, da področje integralne korporativne varnosti v Sloveniji ni podrobno raziskano. V prihodnje bo treba dobro prakso iz tujine prenesti v Slovenijo, hkrati pa je priporočljivo, da se tako v teoriji kot v praksi začne z razvijanjem omenjenega področja. Da bi zagotovili ustrezno integralno korporativno varnost, mora organizacija sprejeti številne ukrepe in aktivnosti. Le ti se morajo nato tudi ustrezno upoštevati in izvajati.

Izvirnost/pomembnost prispevka:

Obravnavanje integralne korporativne varnosti in pregled njenih glavnih delov sta namenjena za usposabljanje strokovne javnosti in seznanitev splošne javnosti.

UDK: 005.922.1

Ključne besede: varnost, korporacije, organizacije, integralna korporativna varnost

Integral Corporate Security

Purpose:

Considerable attention has been devoted to study and research of policing, police organizations, private security and private security services in Slovenia in the last years. The integral corporate security has not received so much attention. The purpose of the paper is to present the basics of integral corporate security and its scope.

Methods:

The integral corporate security was analysed and presented by descriptive methods and the synthesis of acquired and existing knowledge. An overview of literature and laws was made by analysing the content of written sources.

Findings:

The literature review has shown that the integral corporate security has not been studied a lot in Slovenia. It will be necessary in the future to transfer a good practice from abroad to Slovenia. There is a lot of work ahead and it is recommended to start developing this field in practice as well as in theory. To ensure the proper integral corporate security it is necessary for each organization to introduce several measures and activities. Furthermore, they should implement them and the people should consider them.

Originality:

The overview of integral corporate security and the review of its main parts can be used for the training purposes of professional public and to inform the general public about its importance.

UDC: 005.922.1

Keywords: security, corporations, organizations, integral corporate security

1 UVOD

Integralna korporativna varnost skrbi za zagotavljanje varnosti v organizacijah in je opredeljena kot zaščita premoženja in poslovnih procesov v organizaciji, njeni ukrepi pa so tako preventivni kot kurativni. Kot ugotavlja Button (2014), se je v zadnjih tridesetih letih drastično povečalo proučevanje in raziskovanje področja zasebnega varovanja in zasebne varnosti. Raziskovanju področja integralne korporativne varnosti pa je posvečenega manj prostora. Zavedati se moramo, da je raziskovanje področja integralne korporativne varnosti zelo pomembno, saj vpliva tako na organizacijo samo, njeno uspešnost kot tudi na ljudi in njihovo vedenje, ki so v njej zaposleni.

V teoriji in praksi se pojmovanje korporativne varnosti precej razlikuje. Hkrati pa se razlikujejo tudi mnenja, kaj vse se uvršča v njen obseg. Po mnenju Walbya in Lipperta (2014) se (integralna) korporativna varnost pojavlja kot primarna oblika varnosti 21. stoletja. Njuna opredelitev pojma je zelo ohlapna. Navajata, da je korporativna varnost zagotavljanje varnosti, ki si prizadeva za doseganje organizacijskih ciljev organizacij. Gerginova (2016) opredeli korporativno varnost kot zaščito lastnine in poslovnih procesov, s čimer bi lahko preprečili in zmanjšali materialne izgube in poskrbeli za varnostne interese lastnikov, zaščitili dobiček in premoženje pred različnimi nevarnostmi. Njeno mnenje je, da obstaja precejšnja razlika v določitvi izraza korporativna varnost s praktičnega in teoretičnega vidika. Kljub temu pa sta si tako teorija kot praksa enotni, da izvajanje korporativne varnosti zahteva stalen nadzor in izdelavo analize kriminalitete, razvoj programa za preprečevanje kriminalitete ter programa za izobraževanje in razvoj varnostne kulture zaposlenih ter doseganje zanesljivosti

poslovanja in uspeha organizacije. Cubbage in Brooks (2012) menita, da je naloga korporativne varnosti odkrivanje goljufij in kaznivih dejanj ter preučevanje konkretnih kriznih primerov organizacije, ki bi se jih morali strokovnjaki s področja korporativne varnosti organizacije zavedati in zagotoviti učinkovito zaščito ljudi in sredstev. Markelj in Završnik (2016) poudarita, da je korporativna varnost sistem za zagotavljanje notranje varnosti podjetja in obsega vrsto ukrepov od pravnih, organizacijskih, funkcionalnih, tehničnih in kadrovskih v skrbi za ohranitev reda, spoštovanje zakonov in internih predpisov ter varnost ljudi in premoženja v podjetju. Po njunem mnenju je namen korporativne varnosti identificirati in izvesti vse potrebne sistemske ukrepe za obvladovanje varnostnih tveganj v posamezni organizaciji in predstavlja eno od funkcij korporacije. Zaradi digitalizacije poslovnih procesov gospodarskih in drugih subjektov korporativna varnost neizogibno vključuje tudi kibernetske varnostne vidike.

Gerginova (2016) izpostavi, da kljub temu, da je kar nekaj avtorjev poskusilo opredeliti korporativno varnost, primanjkuje natančna opredelitev tega pojma. Mnenje Walbyja in Lipperta (2014) je, da je opredelitev korporativne varnosti izziv, s čimer se strinjamo tudi mi. Zato je namen prispevka analizirati in predstaviti integralno korporativno varnost in njen obseg. Pri tem bomo uporabili deskriptivno metodo in sintezo pridobljenih ter obstoječih znanj. Z analizo vsebine pisnih virov bomo naredili pregled domače in tuje literature ter zakonov, ki so pomembni za področje obravnavane tematike. V prispevku bo predstavljeno, kako zagotoviti zakonito in nemoteno poslovanje organizacij, katera zakonska določila so nam pri tem v pomoč, kaj je varnostna kultura organizacij in kako poteka integralno zagotavljanje varnosti v organizaciji.

2 ZAGOTAVLJANJE ZAKONITEGA IN NEMOTENEGA POSLOVANJA ORGANIZACIJ

Vsaka organizacija ima oddelek, odsek, sektor ali službo, ki se ukvarja z zagotavljanjem varnosti. Večje organizacije in korporacije imajo varnostno službo kot samostojno enoto, medtem ko jo imajo manjše organizacije kot del nekega splošnega upravljavskega oddelka. Glede na obsežen pravni sistem na področju zagotavljanja varnosti organizacij lahko predpostavimo, da je izvajanje zakonskih določil v organizaciji učinkovito, vendar, kot je navajal že Vršec (1993), temu ni tako. Razlog za to vidi v tem, da je ogromno predpisov v celoti neuravnoteženih z gospodarskimi interesi ter potrebami. Poleg tega se v praksi pojavljata dva problema. Prvi se nanaša na tiste, ki bi morali upoštevati pravne norme oziroma zakonska določila (organizacije ter odgovorne osebe v njih za dosego ciljev izkoriščajo pravne praznine); drugi pa na tiste, ki bi morali zagotavljati izvajanje pravnih norm (organi nadzora), ki pa so zaradi ohlapnosti pravnega sistema, odsotnosti varnostne politike, nizke motivacije in neustrezne organiziranosti premalo učinkoviti. Bistveni vzrok je v tem, da pripravljavci pravnih aktov pomanjkljivo preučijo problematiko področja, za katerega pripravljajo predpis ter pri tem ne upoštevajo raziskovalnih izsledkov. Nadaljnje vzroke lahko pripišemo nizki pravni ter poslovni morali, šibki varnostni kulturi udeležencev organizacije

ter slabemu profesionalnemu nastopanju organov nadzora. Sprejemanje predpisov po hitrem postopku, prepočasen pravosodni sistem in neusklajen pristop organov nadzora dodatno pripomorejo k neučinkovitosti pravnega sistema. Za izkoriščanje pravnega nereda ne moremo kriviti zgolj organizacij in zaposlenih, ki si želijo delovati po ekonomskih ter tržnih načelih. Ko bo pravni sistem poenostavljen ter cenejši za izvajanje, ko bo nanj naravnana varnostna politika oziroma ko bodo organi nadzora nastopali v visoki meri profesije, bodo zagotovljeni tudi pogoji za ustvarjalno vedenje organizacij ter zaposlenih v njih.

Da pridobimo podatke o tem, kako ima organizacija opredeljeno področje varovanja, je treba pregledati statute, obstoječe pravilnike ter druge notranje akte. Statuti bi morali določati varnostne koncepte, temeljno varnostno politiko in izhodišča za razvojno varnostno politiko. Vsi prej našteti dejavniki so osnova za izdelavo varnostnega programa oziroma izdelavo načrta varovanja organizacije. Podrobnejša pravila obnašanja na področju varovanja organizacije določajo pravilniki ali skupek več pravilnikov. Obstajajo pravilniki o organizaciji ter delovanju varnostne službe, varovanju poslovnih skrivnosti, varstvu pri delu, varovanju premoženja, notranji kontroli ter reviziji, požarnem varstvu in drugi.

Pri tem ima ključno vlogo svetovalec, ki prouči njihovo zanesljivost, pomembnost ter uporabnost v praksi varovanja organizacije. Na podlagi tega pripravi metodološke ter vsebinske podlage za izdelavo enotnega pravilnika o varovanju organizacije. Vršec (1993) navaja, da morata biti tako načrt varovanja organizacije kot tudi pravilnik o varovanju organizacije okvir dejanske ogroženosti oziroma varnostnih potreb organizacije. Dosežena mora biti tudi pravilna raven varnostne kulture zaposlenih. Posebno pozornost je treba nameniti definiranju pravil zaščite intelektualne lastnine, pravil zaščite pri delu, protipožarne zaščite, industrijske lastnine in poslovnih skrivnosti.

2.1 Zakonska določila

Podjetje je pravna oseba, ki opravlja gospodarsko dejavnost zaradi pridobivanja dobička. Z gospodarsko dejavnostjo so po Zakonu o podjetjih (1988, 1. člen) mišljeni proizvodnja ter promet blaga in prav tako opravljanje storitev na trgu. Posamezne oblike zaščite v organizacijah urejajo zakoni ter drugi predpisi, in sicer predpisi s področja zaščite premoženja, ekologije, logistike, varstva pri delu, industrijske lastnine, obrambe, požarnega varstva, ergonomije ter drugih področij varovanja.

Zakon o industrijski lastnini (ZIL-1, 2006) je predpis sistemske narave in celovito ureja skoraj celotno področje industrijske lastnine, in sicer: sodno varstvo patentov, geografske označbe, pridobitev, znamke, modele in trajanje. Industrijska lastnina se v najširšem pomenu besede ne nanaša samo na ozek segment, torej tako rečeno le na industrijo ter trgovino, ampak na panogo kmetijskih ter ekstrativnih industrij in na vse pridobljene ali naravne proizvode (vino, tobačni listi, živina, sadje, pivo, cvetje, moka, mineralne vode itd.). Z gospodarskega vidika je ena od najpomembnejših funkcij pravic industrijske lastnine konkurenčna funkcija.

Zasebno varovanje je v Sloveniji svojo »domovinsko pravico« pridobilo z letom 1994, ko je bil sprejet Zakon o zasebnem varovanju in obveznem organiziranju

službe varovanja (ZZVO, 1994). Razvoj na tem področju se je začel že prej, vendar v drugi obliki ter v drugih dimenzijah. Z zasebno varnostjo razumemo tisto stanje, občutje ter potrebo, ki ga dosežemo z dodatnim varstvom, se pravi zasebnim varstvom. Bistvena naloga je, da dopolnjuje varstvo, ki ga zagotavlja sodobna družba z nacionalnovarnostnim sistemom. Pri zasebno varnostni dejavnosti je treba opozoriti na pomemben element profesionalizacije, kajti posamezniki ali organizacije veljajo za odjemalce uslug ter storitev (potrošniki). Pomembno je, da imajo izvajalci te dejavnosti znanje tudi o potrošnikovih potrebah. Usluge izvajalcev zasebne dejavnosti vedno sledijo interesom prizadetih oziroma oškodovanih strank, delovna uspešnost pa se meri z učinkovitim doseganjem ciljev, in sicer tako, da s primernim upravljanjem aktivnosti dosežemo minimalizacijo stroškov in ravno nasprotno maksimilizacijo rezultatov za naročnike oziroma organizacijo (Modic, Lobnikar in Dvojmoč, 2014). Pri tem je pomembno poudariti, da so vložki na področju zagotavljanja korporativne varnosti investicija v obvladovanje ter učinkovitost delovanja organizacije in ne nepotreben strošek. To pomeni, da je treba uveljavljati kakovostne rešitve, ki v določenih primerih niso omejene na izbiro najcenejših ponudnikov ter storitev, saj lahko ti dolgoročno povzročijo neizmerno več stroškov (Čaleta, 2011). Zasebno varovanje je sčasoma postalo velik akter na varnostnem tržišču. Po skoraj desetih letih skokovitega razvoja je zasebno varovanje doseglo enega izmed svojih največjih uspehov, ko je bil leta 2003 sprejet Zakon o zasebnem varovanju (ZZasV, 2003). Leta 2011 je v veljavo stopil nov Zakon o zasebnem varovanju (ZZasV-1, 2011), ki je v veljavi še danes. Kot navajajo Modic et al. (2014), je nov zakon prinesel številne spremembe ter novele v primerjavi z zakonom iz leta 2003. V njem je opredeljenih osem oblik varovanja in vse zahtevajo licence, ki jih podeljuje Ministrstvo za notranje zadeve RS.

Neizogibno je dejstvo, da ne smemo funkcije strateškega varnostnega menedžmenta zamenjevati z dejavnostjo, ki jo ponujajo zasebnovarnostne službe v okviru zavarovanja ljudi ter premoženja. Čaleta (2011) izpostavi, da predstavlja največjo nevarnost za nesistemske pristope na področju celostnega obvladovanja varnostnih tveganj v organizacijah ravno združevanje teh funkcij v rokah zasebnovarnostnih služb, ki hitro izgubijo skrb za naročnika ter jih vodi le še skrb za lastni dobiček. Prav zaradi te nevarnosti mora biti strateški korporativni varnostni menedžer oseba, ki je v tem razmerju naročnika ter izvajalcev varnostnih storitev neodvisen ali objektiven ter lastniku pomaga k učinkoviti izbiri najboljšega ponudnika za zagotavljanje posameznih varnostnih storitev. Enakega mnenja sta tudi Brooks in Corkill (2014). Ena izmed njegovih ključnih nalog je tudi, da skrbi za sistemski nadzor nad izvajanjem in delovanjem varnostnih storitev.

Leta 1994 je bil sprejet tudi Zakon o detektivski dejavnosti (ZDD, 1994). To je pomenilo konec državnega monopola na varnostnem področju. Nadstandard varnosti je tako postal »tržno blago«, ki si ga zainteresirani lahko »kupijo« na trgu zasebnih varnostnih storitev. Nov Zakon o detektivski dejavnosti (ZZD-1, 2011) je bil sprejet leta 2011. Le-ta ne odstopa od ciljev ter načel dotedanjih predpisov, vendar pomeni nadaljevanje dotedanje prakse. Prinesel je spremembe pri opravljanju dejavnosti, saj je za gospodarske družbe ter fizične osebe odpravljal nepotrebne administrativne ovire, obenem pa je bolj natančno opredelil pogoje za opravljanje dejavnosti. Po besedah Savskega, Grilca, Jarca in Meleta (2012) so

bile odpravljene nekatere nejasnosti oziroma pomanjkljivosti, ki so se pokazale pri uporabi prej veljavnih zakonskih aktov in na katere je opozarjala sodna praksa. ZZD-1 (2011) je natančneje določil pogoje za opravljanje detektivske dejavnosti, varnostne zadržke ter varnostno preverjanje in merila za odločanje o varnostnih zadržkih, določena je obveznost usposabljanja pred opravljanjem detektivskega izpita in možnost podelitve javnega pooblastila, razmejene so pristojnosti med detektivsko zbornico RS in ministrstvom, pristojnim za notranje zadeve, določeno je, da se detektivska dejavnost lahko izvaja le na podlagi sklenjene pogodbe in pooblastila stranke, opredeljena so bila delovna področja detektivov, taksativno so določena upravičenja, ki jih detektiv lahko uporablja pri svojem delu, določene so prepovedi in dolžnosti detektivov pri opravljanju detektivske dejavnosti, določene so obveznosti pri zavarovanju odgovornosti, natančneje so opredeljeni pogoji za prenehanje opravljanja detektivske dejavnosti, začasni, pogojni in trajni odvzem licence ter službene izkaznice, natančneje so določeni pogoji za opravljanje detektivske dejavnosti tujih detektivov, določene so naloge in status pristojnega organa (tj. Detektivske zbornice RS), določeni so pogoji za ustanavljanje gospodarskih družb za opravljanje detektivske dejavnosti in določena sta inšpekcijski organ ter njegova vloga pri nadzoru nad izvajanjem ZDD-1 (2011). Tudi na področju detektivske dejavnosti se je mednarodnopravna primerjava zakonodajnopravne ureditve združila v tri osnovne zahteve. Obveznost varovanja posameznikovih človekovih pravic in svoboščin, vzdrževanja državnega monopola nad uporabo ukrepov ter definicija javne/zasebne dejavnosti na področju detektivske dejavnosti; določitev zahtev oziroma omejitev v javnem interesu, kot so zadržki in primernost za opravljanje detektivske dejavnosti, obveznost zavarovanja dejavnosti in nadzora nad uporabo ukrepov; določitev minimalnih etičnih in strokovnih standardov detektivske dejavnosti z organiziranjem obveznega usposabljanja pred opravljanjem detektivskega izpita in prepoved opravljanja detektivske dejavnosti tistim, ki so pred določenim časovnim obdobjem opravljali delo policista ali druge poklice s posebnimi pooblastili (Savski et al., 2012).

Leta 2001 je začel veljati Zakon o tajnih podatkih (ZTP, 2001), s čimer je bila zaključena naloga, začeta julija 1998. Namreč takrat je vlada po obravnavi analize stanja varovanja tajnih podatkov z delovnega področja državnih organov, ki jo je pripravilo Ministrstvo za notranje zadeve, ter spoznanju, da so razmere daleč od zadovoljivih, sklenila, da je treba varovanje teh podatkov urediti z zakonom. Pripravo predloga zakona je dodelila Ministrstvu za notranje zadeve. Zakon o tajnih podatkih (ZTP, 2001) je bil, po navajanju Antončiča (2001), prvi tovrstni zakon v zgodovini pravnega reda Republike Slovenije, vključno z obdobjem nekdanje skupne države. Po Zakonu o tajnih podatkih se določajo skupne osnove enotnega sistema odločanja, varovanja ter dostopa do tajnih podatkov z delovnega področja državnih organov Republike Slovenije, ki se nanašajo na javno varnost, obrambo, zunanje zadeve ali obveščevalno in varnostno dejavnost države, ter prenehanje tajnosti takšnih podatkov. Po omenjenem zakonu se morajo ravnati različni organi, in sicer državni organi, organi lokalnih skupnosti, nosilci javnih pooblastil in drugi organi, gospodarske družbe, organizacije in posamezniki v teh organih, dobavitelji, izvajalci gradenj ali izvajalci storitev (Zakon o tajnih

podatkih, 2001, 1. člen). Vlada Republike Slovenije je morala za izvajanje določenih nalog s področja varovanja tajnih podatkov, predpisanih v zakonu, ter s predpisi, sprejetimi na njegovi podlagi, najkasneje v 6 mesecih po uveljavitvi zakona ustanoviti Urad Vlade Republike Slovenije za varovanje tajnih podatkov, katerega naloge so spremljanje, določanje ter varovanje tajnih podatkov ter skrb za razvoj ter uveljavljanje fizičnih, organizacijskih ter tehničnih standardov varovanja tajnih podatkov v državnih organih, organih lokalnih skupnosti, pri nosilcih javnih pooblastil ter v organizacijah, ki pridobijo oziroma razpolagajo s tajnimi podatki; pripravljanje predlogov predpisov, potrebnih za izvajanje obravnavanega zakona, skrb za izvrševanje sprejetih mednarodnih obveznosti ter mednarodnih pogodb o varovanju tajnih podatkov in na tem področju sodelovanje z ustreznimi organi tujih držav ter mednarodnih organizacij, vodenje evidence izdanih dovoljenj, podajanje mnenj k skladnosti splošnih aktov o določanju, varovanju ter dostopu do tajnih podatkov v obravnavanem zakonu, predlaganje ukrepov za izboljšanje varovanja tajnih podatkov, vodenje evidence oseb iz 4. odstavka 23. člena Zakona o tajnih podatkih, opravljanje drugih nalog, ki so določene s predpisi, sprejetimi na podlagi obravnavanega zakona, in prav tako koordiniranje delovanja državnih organov, pristojnih za varnostno preverjanje (Antončič, 2001).

Upravni delavci imajo zaradi dela, ki ga opravljajo, pomembno vlogo na področju varovanja zaupnih oziroma tajnih podatkov. Gre namreč za podatke, ki so strateško pomembni za poslovanje ter obstoj organizacije, prav tako pa so pomembni za poslovne partnerje, s katerimi organizacija sodeluje. Kot izpostavi Stare (1995), lahko pride v primeru zlorabe tajnih podatkov do zmanjšanja poslovne uspešnosti, kar pa privede do prekinitve gospodarskih vezi med poslovnimi partnerji, odpuščanje zaposlenih ali v najhujši situaciji celo do propada organizacije. Prav tako ima vse skupaj zelo negativne posledice za državo, saj začne prihajati do skokovitega porasta nezaposlenega prebivalstva, povečanje socialnih nemirov itd. Način varovanja tajnih podatkov določi vsaka organizacija zase in obsega organizacijske ter pravne postopke. S tem poskuša preprečiti dostop nepooblaščenim osebam, obdelavo ter spreminjanje podatkov kakor tudi poškodovanje, uničenje ter nepooblaščen iznos iz organizacije. V sklopu tega je vseeno, ali gre za različne baze podatkov, evidence ali registre oziroma ali so ti podatki zbrani na papirju ali v/na kakšnem drugem mediju (Stare, 1995).

Zakon o tajnih podatkih (ZTP, 2001) je od vseh državnih organov zahteval, da so zagotovili, da so vsem zaposlenim, ki morajo zaradi delovnih funkcij imeti dostop do tajnih podatkov, izdana dovoljenja za dostop do tajnih podatkov. Delavcem ter funkcionarjem, ki tega dovoljenja nimajo, je dostop do tajnih podatkov onemogočen. Poleg tega so morali sprejeti predpise ter se organizacijsko prilagoditi za njegovo uveljavitev oziroma obstoječe akte ter organizacijo svojega poslovanja uskladiti z določbami tega zakona. Tajnim podatkom, ki jim je bila oznaka stopnje tajnosti določena pred uveljavitvijo zakona, so morali določiti stopnjo tajnosti skladno z Zakonom o tajnih podatkih, v nasprotnem primeru jim je tajnost prenehala. Lalić (2003) je mnenja, da je realnost v državni upravi takšna, da ima posameznik v večini organov državne uprave le redko opravka s tajnimi podatki in če bi se Zakon o tajnih podatkih (2001) izvajal po določenih načelih, posameznik pa ne bi privolil na varnostno preverjanje, bi bila državna uprava paralizirana.

Pravica do varstva osebnih podatkov je urejena že v Ustavi Republike Slovenije (1991), ki v 38. členu izrecno določa, da je zagotovljeno varstvo osebnih podatkov in da je prepovedana uporaba osebnih podatkov v nasprotju z namenom njihovega zbiranja. Zbiranje, obdelovanje, namen uporabe, nadzor ter varstvo osebnih podatkov pa so določeni v Zakonu o varstvu osebnih podatkov (ZVOP-1, 2007). Vsakdo se ima pravico seznaniti z zbranimi osebnimi podatki, ki se izrecno nanašajo nanj, prav tako pa ima pravico do sodnega varstva ob njihovi zlorabi. Človekova pravica do ohranjanja zasebnosti osebnih podatkov v sodobnem svetu pa je ogrožena zaradi rabe kibernetskega prostora in komuniciranja v njem.

Stare (1995) izpostavi, da bi se morale organizacije zavzemati za preventivno ukrepanje ter ureditev stanja na področju varovanja poslovne skrivnosti, saj je morebitne zlorabe zelo težko dokazovati. Prav tako meni, da bi morala, za ureditev stanja na tem področju, vsaka organizacija sprejeti pisni sklep o varovanju tajnih podatkov in natančno definirati način določanja vsebine ter stopnje zaupnosti podatkov. V sklopu ukrepov ter postopkov za varovanje tajnih podatkov morajo v organizaciji obravnavati splošne varnostne ukrepe, varovanje prostorov, tehnične opreme ter programske opreme. Organizacija mora definirati način ravnanja s podatki, ki vsebujejo poslovno skrivnost in odgovornost za izvajanje varnostnih ukrepov ter postopkov. Neizogibno pozornost morajo nameniti nadzoru nad izvajanjem varnostnih ukrepov, saj iz prakse sklepamo, da je le-tega v slovenskih organizacijah premalo.

Poleg že omenjenih zakonov je bil leta 2016 oblikovan tudi Predlog Zakona o kritični infrastrukturi (2016). Bistveni namen Zakona o kritični infrastrukturi je urediti ugotavljanje ter določanje kritične infrastrukture Republike Slovenije, načrtovanje ter urejanje zaščite kritične infrastrukture, urejanje pristojnosti in odgovornosti organov kot tudi organizacij na omenjenem področju ter obveščanje, poročanje in zagotavljanje podpore pri odločanju, varovanju podatkov ter nadzoru na področju kritične infrastrukture (Predlog Zakona o kritični infrastrukturi, 2016, 1. člen). Temeljni namen predloga zakona je sistemsko urediti sistemske temelje področja kritične infrastrukture, ki vključuje ugotavljanje ter določanje kritične infrastrukture in njeno zaščito. Glede na opisano si lahko razlagamo, da obsega zaščita kritične infrastrukture vse aktivnosti, ki prispevajo k neprekinjenosti oziroma celovitosti njenega delovanja. Osnovni cilji Predloga Zakona o kritični infrastrukturi (2016) so predvsem z ustreznim celovitim predpisom urediti področje kritične infrastrukture državnega pomena, torej tudi »nacionalno« kritično infrastrukturo, vse organe oziroma organizacije pri zagotavljanju neprekinjenega ter celovitega delovanja kritične infrastrukture zavezati k spoštovanju istih splošnih načel, vsem organom oziroma organizacijam, ki delujejo na področjih, ki so za slovensko družbo posebej pomembna, naložiti, da pri svojem delu upoštevajo tudi zahteve glede zagotavljanja konstantnega oziroma stalnega delovanja (kritične) infrastrukture, torej vidik zaščite kritične infrastrukture, z normativnim ukrepom prispevati k dvigu ravni odpornosti slovenske družbe na sodobne varnostne grožnje ter tveganja, naložiti dopolnitev normativne urejenosti ali sploh normativno ureditev, če le-ta še ne obstaja, v posameznih sektorjih kritične infrastrukture z vidika zaščite kritične infrastrukture in med organi ter organizacijami, ki delujejo na področjih sektorjev

kritične infrastrukture, vzpostaviti primerna razmerja, predvsem z vidika delitve njihovih pristojnosti ter odgovornosti za zaščito kritične infrastrukture (Predlog Zakona o kritični infrastrukturi, 2016).

Predlog Zakona o kritični infrastrukturi (2016) je Vladi Republike Slovenije kot tudi ministrstvom v vlogi nosilcev kritične infrastrukture doprinesel nove ter jasno določene pristojnosti, odgovornosti ter obveznosti pri zaščiti obravnavanega področja. Ob tem bodo organi državne uprave ter izvršne veje državne oblasti prispevali svoj del k zagotavljanju konstantnega delovanja kritične infrastrukture. To delovanje je definitivno v javnem interesu, saj gre za infrastrukturo, s katero se zagotavljajo zmogljivosti ter storitve, ki so bistvenega pomena za državo in bi prekinitev njihovega delovanja imela resne posledice na nacionalno varnost, gospodarstvo, zdravje, varnost, ključne družbene funkcije, zaščito in družbeno blaginjo (Predlog Zakona o kritični infrastrukturi, 2016). Načela, na katerih temelji zaščita kritične infrastrukture, so kot nekakšne usmeritve pri izvajanju tega področja. Ta načela so načelo zaščite pred različnimi vrstami nevarnosti, ki zahteva, da pristojni organi ter organizacije pri zagotavljanju neprekinjenega delovanja kritične infrastrukture upoštevajo različne vrste nevarnosti; načelo izmenjave podatkov oziroma informacij ter varovanja podatkov, ki od pristojnih organov oziroma organizacij zahteva redno, pravočasno ter na zaupanju temelječo izmenjavo informacij ob hkratnem varovanju podatkov, povezanih s kritično infrastrukturo, v skladu s predpisi, ki urejajo varovanje tajnih podatkov; načelo celovitega pristopa, ki zahteva, da se v zaščito obravnavanega področja pred, med ter po motnjah v delovanju oziroma prekinitvi delovanja kritične infrastrukture vključuje vse pristojne organe oziroma organizacije ter pri tem upošteva različne vrste nevarnosti, izhaja iz ocene tveganja ter upošteva soodvisnost sektorjev kritične infrastrukture ter njihov medsebojni vpliv; načelo stalnega načrtovanja zaščite, ki zahteva, da je načrtovanje zaščite kritične infrastrukture podprto s stalnim procesom ocenjevanja tveganja za delovanje ter presojo ustreznosti ukrepov za njeno zaščito; in navsezadnje načelo odgovornosti, po katerem so za delovanje kritične infrastrukture neposredno odgovorni upravljavci le-te, za krepitev zaščite kritične infrastrukture pa vsi pristojni organi oziroma organizacije.

Ob tako širokem naboru zakonodaje, ki je potrebna za ustrezno zagotavljanje integralne korporativne varnosti, je treba upoštevati tudi zakonodajo in dognanja na področju informacijske varnosti, zavarovalništva, bančnega sistema, varstva in zdravja pri delu, raznih standardov kakovosti in še mnogo drugega.

2.2 Zaščita poslovnih skrivnosti

V Zakonu o gospodarskih družbah (ZGD-1, 2006) se za poslovno skrivnost štejejo podatki, za katere tako določi družba s pisnim sklepom. Z omenjenim sklepom morajo biti seznanjeni družbeniki, delavci, člani organov družbe ter druge osebe, ki morajo varovati poslovno skrivnost (ZGD-1, 2006, 39. člen, 1. odstavek). Poslovno tajnost pa definira Zakon o podjetjih (ZPOd, 1988, 176. člen), ki jo opredeli kot listine ter podatke, določene s statutom oziroma pravili ali kakšnimi drugimi samoupravnimi splošnimi akti oziroma splošnimi akti podjetja, katerih posredovanje nepooblaščeni osebi bi bilo v nasprotju s poslovanjem podjetja in bi škodovalo njegovim interesom ter poslovnemu ugledu, če z zakonom ni določeno drugače.

Zakonodajalec s svojimi zakonskimi določili v zvezi s poslovno skrivnostjo organizacijam pomaga ščititi njihove poslovne skrivnosti, kar je tudi v interesu države. Kop (1995) navaja, da nam država pomaga ščititi poslovne skrivnosti le v primeru, ko gre zakonske poslovne skrivnosti in če izpolnjujejo določene pogoje. Z zakonom država določi, kako definira poslovno skrivnost, pogojev, ki se morajo izpolnjevati, pa ne navaja nikjer. To ne pomeni, da ti pogoji ne obstajajo in da niso pomembni. Država jih sicer res ne navaja, jih je pa oblikovala sodna praksa na podlagi dojemanja bistva zakonskih poslovnih skrivnosti ter osnovnega namena pomoči države. Pogoji, ki jih morajo izpolnjevati zakonske poslovne skrivnosti, so: zadeva mora biti dejstvo in ne domneva ali sklepanje, zadeva mora biti relativno oziroma absolutno neznana, torej pri njej ne moremo govoriti o javni skrivnosti. Krog ljudi, ki to zadevo pozna, mora biti bolj ali manj sklenjen (krog je še vedno sklenjen v primeru, ko smo morali svojo poslovno skrivnost razkriti poslovnemu partnerju, ta pa je sprejel pravno veljavno obveznost, da jo bo varoval), interes organizacije mora biti legitimen, kar pomeni, da je organizacija prišla do poslovne skrivnosti na pravno nesporen način, dano mora biti razmerje do proizvodnih ter poslovnih zadev. To razmerje mora biti krogu poznavalcev poslovne skrivnosti znano, volja organizacije, da naj bo zadeva tajna, mora biti jasno izražena ter poznavalcem poslovne skrivnosti znana. Navedeno idejo organizacija izvede tako, da podatek oziroma informacijo jasno razglasi za poslovno skrivnost, organizacija pa mora imeti upravičen interes, da se zadeva ohrani v tajnosti, recimo: zaradi gospodarskih koristi (Kop, 1995). O zaščiti poslovne skrivnosti govorimo takrat, ko nekdo, ki poslovne skrivnosti ne pozna, skrbi za to, da poslovna skrivnost ne bi prešla v roke tretje osebe. Kot imetniki poslovnih skrivnosti imamo na razpolago mnogo možnosti za zaščito podatkov oziroma informacij. To so lahko take, ki skušajo preprečiti vse mogoče načine prehoda poslovnih skrivnosti v neprave roke oziroma k tretjim osebam, ali pa take, ki po izvedenem prehodu skušajo preprečiti oziroma vsaj zmanjšati škodo. Poslovne skrivnosti lahko zaščitimo z naslednjimi ukrepi, ki so kadrovske narave, recimo: odklonitev zaposlitve delavca, ki je pri prejšnjem delodajalcu izdal njegovo poslovno skrivnost; pravne narave, recimo: določilo o dolžnosti varovanja poslovnih skrivnosti v pogodbi o delu; tehnološke narave, recimo: fizična preprečitev dostopa nepoklicanim v razvojni laboratorij; organizacijske narave, recimo: skrb za dobro poučenost sodelavcev o zadevah v zvezi z varovanjem poslovnih skrivnosti; elektronski prenos informacij (kot je npr. šifriranje), elektronska obdelava informacij, recimo: preprečitev pristopa do posameznih poslovnih skrivnosti neupravičenim osebam (Kop, 1995).

Za učinkovito zaščito je pomembno prepletanje več pogojev, bistvenega pomena pa so po navajanju Kopa (1995) dobro ozračje v organizaciji, dobra poučenost, dober koncept za varovanje ter zaščito in zagotovitev ugodnih pogojev za učinkovitost ukrepov, ki so pravne narave.

2.3 Poslovna etika in integriteta

Etična vloga menedžerja je tisto, kar strokovnjaki imenujejo etično voditeljstvo. To razumemo kot kombinacijo med moralno osebnostjo (lastnosti menedžerja kot človeka) ter moralnim menedžerjem (njegovo funkcijo ali vlogo v organizaciji).

Moralna oseba je tista, ki ima integriteto in je prav tako poštena ter zaupanja vredna. Integriteta pa ne vsebuje samo pravičnosti ter poštenja, ampak vključuje tudi skrb za zdravje celotne organizacije, ki jo nekdo upravlja. Z drugimi besedami integriteta pomeni tudi, da se organizacija ravna po etičnih načelih ter pravilih in da je moralna osebnost tista, ki ima osebno integriteto in je oseba vredna zaupanja (Vadnjal, 2014). Integracija visoke stopnje varnega vedenja ne vpliva zgolj na zaposlene v organizaciji, vendar prav tako strmi k dvigu varnega vedenja organizacij, ki sodelujejo z organizacijo, v kateri je formirana varnostna kultura. Z visoko stopnjo zavedanja organizacija lažje obvladuje široko področje varnostnih dogodkov (Vedenik in Miketić-Curman, 2013).

Menedžerja, ki ne razume pomena korporativne varnosti in si jo interpretira zgolj kot strošek, težko označimo kot zaupanja vredno osebo. Na podlagi tega lahko sklepamo, da je pripravljen prihodnja tveganja vrednotiti zgolj ekonomsko. Vadnjal (2014) izpostavi, da velika večina menedžerskih nagrajevanj izhaja iz pravno utemeljenega zneska čistega dobička tekočega leta, ki se danes ponekod obračunavajo celo kvartalno. Problemi etičnega odločanja nastopijo takrat, ko odločitve vsebujejo moralni konflikt. Ta se pojavi takrat, ko se mora menedžer odločiti med vsaj dvema navidezno slabima izbirama oziroma takrat, ko se pojavijo večplastne etične odločitve, ki so pogosto v medsebojnem konfliktu interesov. Skupina strokovnjakov je po mnenju Vadnjala (2014) menedžerjem olajšala odločitve s tem, ko je pripravila določen okvir, ki temelji na idejah filozofov ter etikov. Odločitve menedžerjev lahko razdelimo v štiri sklope (Vadnjal, 2014):

- *pravice in dolžnosti:* gre za pravila, ki so na nacionalni ravni v obliki zakonov ter drugih predpisov. Tako recimo delovnopravna zakonodaja predpisuje pravice, ravno tako tudi delno dolžnosti delavcev in prav tako dolžnosti ter deloma tudi pravice delodajalcev. Na mednarodni ravni tak okvir predstavljajo različne mednarodno predpisane deklaracije, na primer: Deklaracija Združenih narodov o človekovih pravicah;

- *utilitarianizem*: usmeritev, da naj bo odločitev taka, da bo čim bolj ugodna za čim širši krog zainteresiranih ljudi. Gre za analizo stroškov ter koristi, ki jo je težko narediti v številkah, zato je v veliki meri odvisna od razvitih sposobnosti tistega, ki mora presojati, saj gre za celovito oziroma vsestransko vprašanje: »kdo vse bo prizadet zaradi odločitve?« ter »kakšna je škoda ali korist za posameznika ali celotno skupino?«;

- *pravičnost:* tu je treba upoštevati, da moramo vse, ki jih bo odločitev doletela, obravnavati enakopravno ter jim dajati enake možnosti. Ta koncept definiramo kot kategorični imperativ, ki ga lahko pojasnimo z vprašanjem: »ali lahko neka odločitev kasneje postane univerzalno pravilo v podobnih primerih?«;

- *čuvanje povezav*: gre za koncept, kako odločitve vplivajo na odnose med posameznimi skupinami oziroma obratno (ali odnosi vplivajo na odločitve). Tipičen primer neetičnega ravnanja s tega vidika je dajanje prednosti zaradi sorodstvenih povezav. Podobno se dogaja, ko v nekaterih organizacijah zaščitijo dolgoletne uslužbence itd.

Mnoge velike organizacije imajo interna pravila obnašanja, ki menedžerjem pomagajo pri odločitvah v smislu etičnih dilem oziroma moralnih konfliktov. Etično vodstvo mora delavcem zagotavljati sistemsko perspektivo, kar pomeni, da

organizacija računa na njih. Se pravi, da se bodo delavci osebnostno ter strokovno razvijali z organizacijo in prav tako organizacija z njimi. Zaposlenim je treba dati vedno več možnosti odločanja ter tako spodbujati in razvijati individualno odgovornost, ki bo temeljila na resnici, integriteti ter poštenosti. Takšen odnos menedžerjev na dolgi rok spodbuja konstruktiven odnos med vsemi deležniki v organizaciji. Pomembno je, da etični voditelj doseže občutek predanosti organizaciji ter skupnemu cilju, tako da poudarja in spodbuja vrednote, kot so: držanje obljub, smiselno postavljanje zaposlenim nujne prioritete ter spodbujanje njihovega kreativnega vključevanja v procese namesto izključevanja podrejenih iz kakršnihkoli možnosti odločanja (Vadnjal, 2014).

2.4 Varnostna kultura organizacije

Varnostna kultura, kot del organizacijske kulture, po mnenju Lobnikarja, Čalete, Žaberla, Anžiča in Rančigajeve (2009) tvori pomemben segment v vzpostavljanju učinkovitih mehanizmov v okoljih, kjer se zaposleni srečujejo z obdelavo in varovanjem tajnih podatkov. Varnostno kulturo lahko opredelimo tudi kot védenje pripadnikov določene organizacije o njihovih pravicah, obveznostih in njihovemu uveljavljanju. Tisti, ki pripadajo določeni varnostni kulturi, se zavedajo, kako lahko njihovo védenje vpliva na varnost, in so s svojim zgledom in nasveti pripravljeni izobraževati tiste pripadnike organizacije, ki ne upoštevajo vzorcev varnostne kulture. Varnostno zavedanje preraste v varnostno kulturo tedaj, ko začne skupina varnostne kršitve moralno in socialno dojemati kot nesprejemljive za skupino. Zelo močan dejavnik, ki pogojuje varnostno kulturo, je poleg trajnega izobraževanja tudi osebni zgled, ki ga vodstveni delavci prenašajo na ostale pripadnike organizacije. Zavedati se je treba, da ima vsaka organizacija posebno obliko varnostne kulture, ki je tipična samo za njeno organizacijsko obliko in delovanje. Varnostna kultura kot taka je lahko združevalna ali razdiralna in predstavlja celoten spekter varnostnih navad ter ravnanj, ki se uveljavijo v določeni družbeni skupini. Tako zagotavlja osnovni temelj za preprečevanje varnostno deviantnih pojavov (Lobnikar et al., 2009).

Rančigajeva in Lobnikar (2012) opredelita varnostno kulturo kot odziv skladnih organizacijskih prizadevanj, ko se elemente organizacijske kulture uperi k doseganju varnostnih ciljev. V to je treba vključiti tako člane organizacije kot tudi sisteme in delovno aktivnost. To predstavlja prehod splošnega varnostnega zavedanja v varnostno kulturo in se zgodi v tistem trenutku, ko začne skupina varnostne kršitve dojemati kot nesprejemljive za okolje, v katerem delujejo, in se prične varnostno obnašati. Njuno mnenje je, da je varnostna kultura koncept, ki je definiran na ravni skupine in se nanaša na skupne vrednote članov organizacije.

Varnostna kultura ima zelo velik pomen tudi za ustrezen odnos članov posameznih organizacij do varovanja tajnosti. Odgovornost za razvoj varnostne kulture v organizacijah se po mnenju Rančigajeve in Lobnikarja (2012) nahaja na različnih nivojih vodenja in upravljanja. Zelo veliko vlogo pri povišanju nivoja varnostne kulture in zavedanja, kako pomembno je učinkovito varovanje tajnih podatkov, ima izobraževanje in upravljanje z znanjem. Raven varnostne kulture je pomemben pokazatelj skrite vrednosti organizacije in skrbi za vzpostavljanje učinkovitih mehanizmov obvladovanja in upravljanja z občutljivimi podatki.

Vodstveno osebje si prizadeva doseči varnostno zavedanje preko različnih pristopov zavednega in nezavednega vplivanja na zaposlene. Rančigajeva in Lobnikar (2012) navajata, da le to izvajajo s pomočjo predpisov, varnostne politike, protokolov in standardov. Le ti pa sami po sebi za varno vedenje niso dovolj, kajti na ravnanje z občutljivimi podatki vplivajo tudi osebne predpostavke o varnosti, ki so odraz posameznikovega zaznavanja varnostnih predpisov in dejanskih groženj.

Vsebinski ter strukturni okvir varnostne kulture v organizaciji predstavlja model varnostne politike. Le-ta zajema vse potrebne elemente varovanja organizacije. Vse se začenja s temeljno varnostno kulturo, ki izraža varnostno miselnost, kot so pogledi, stališča, zamisli in nazori o varovanju organizacije, varnostnih interesih ter motivih zaščite. Razvojna varnostna politika je dinamične narave in prav tako je časovno naravnana na 3 do 5 let, odvisno od sprememb v okolju organizacije ter od ocene ogroženosti organizacije. Njen rezultat je razvojni varnostni program kot strateški dokument za vodenje varnostne kulture organizacije. Funkcija razvojne varnostne kulture pa je predvidevanje ter obvladovanje bodočih sprememb na področju varovanja organizacij ter obvladovanje visokih varnostnih ter poslovnih tveganj, ki povzročajo visoke stopnje ogroženosti in znatne škode ter izgube. Osrednja oziroma bistvena ter razvojna varnostna kultura organizacije vpliva na organizacijsko, tehnično, kadrovsko ter logistično strukturo varnostnega sistema (Vršec, 1993). Ko se organizacija loti preureditve varnostnega sistema s pomočjo zunanjega zasebnega varnostnega inženiringa, si mora na novo oblikovati ter sprejeti novo varnostno kulturo oziroma politiko. Le-ta je pogoj za uvajanje ekonomskega gledanja na varovanje organizacije, kajti od varnostnega sistema se pričakujejo tudi določene ekonomske ter druge koristi. K oblikovanju ter sprejemanju varnostne kulture v organizaciji po mnenju Vrška (1993) vplivajo tudi nekateri zunanji legitimni vplivi, kot so trg zaščite (varnostne storitve zasebnega varnostnega sektorja), revizijski, inšpekcijski, davčni ter preiskovalni postopki, veljavna zakonska določila o varovanju organizacije, strokovna pomoč policije in uradna javna varnostna politika parlamenta ter vlade (smernice, priporočila, sklepi in drugi).

Pravilno načrtovano usmerjanje varnostnih dejavnosti k varnostnim ciljem organizacije daje menedžerjem ter vodjem varnostnih služb učinkovito orodje za obvladovanje dejanske, potencialne ter prikrite ogroženosti organizacij. Vzporedno pa omogoča organiziranje najugodnejše zaščite in doseganje najboljše varnostne kulture organizacije (Vršec, 1993).

2.5 Strateško korporacijsko upravljanje

Po mnenju Čalete in Čalete (2013) področje strateškega upravljanja v organizacijah nima predhodnih izkušenj in ustreznih znanj, zato v organizacijah temu področju ne namenjajo ustrezne pozornosti. Če želimo, da ima strategija zaščite v organizaciji svoj smisel ter da bi prispevala k ekonomskim ter drugim učinkom, se je treba vprašati, kaj je za organizacijo strateškega pomena v danih okoliščinah ter v razvojnem pogledu.

Med strateške varnostne probleme Vršec (1993) uvršča varnostno negotovost, varnostno tveganje, (ne)učinkovitost varnostnega sistema, odločitev o tem, koliko

lastne zaščite ter koliko zunanjih varnostnih storitev bo imela organizacija, škodne pojave, ki povzročajo velike škode ter izgube, in neurejen podsistem varnostnih podatkov. Kot strateške varnostne cilje je določil doseganje varnostnih podciljev (zmanjševanje škod ter izgub, več varnostne kulture zaposlenih, ravnotežje, stroški zaščite oziroma koristi zaščite) in doseganje optimalne varnostne ravni v organizaciji. V zvezi z varnostnimi podatki je strateško, da so zaposleni seznanjeni z varnostnimi podatki, ki sprožajo samozaščitno obnašanje, urejen mora biti podsistem varnostnih podatkov, podatki o zaščiti industrijske, intelektualne ter tržne lastnine, o obveščevalni dejavnosti ter o sistemu tehnične zaščite v organizaciji pa morajo biti zaupne narave. Med strateške zaščitne ukrepe uvršča uvajanje zaščitnih izboljšav ter zaščitnih inovacij v varnostni sistem organizacije, temelj varnostne ter ekonomske učinkovitosti varnostnega sistema organizacije so pravočasni preventivni zaščitni ukrepi na vseh varnostno vitalnih delovnih mestih ter procesih in precizna zaščita tistega dela poslovnih skrivnosti, katerih izdaja, prodaja in/ali kraja bi za organizacijo predstavljala veliko škodo ali izgubo.

Področje zagotavljanja varnega delovnega mesta ureja Zakon o varnosti in zdravju pri delu (ZVZD-1, 2011), kjer je v 16. členu zapisano, da je usposabljanje za varno in zdravo delo sestavni del uvajanja v delo. Kot navaja 38. člen ZVZD-1 (2011), mora delodajalec »delavca usposobiti za varno opravljanje dela ob sklenitvi delovnega razmerja, pred razporeditvijo na drugo delo, pred uvajanjem nove tehnologije in novih sredstev za delo ter ob spremembi v delovnem procesu«. Poleg tega mora biti usposabljanje prilagojeno posebnostim delovnega mesta. Usposabljanje izvaja po določilih 29. člena ZVZD-1 (2011) strokovni delavec. Pri usposabljanju je pomembno, da delavec pridobi tista znanja, ki jih potrebuje za varno in zdravo delo na svojem delovnem mestu. Ocena tveganja za delovno mesto mora biti vir podatkov o tem, kakšna znanja in sposobnosti delavec potrebuje, da bo svoje delo lahko varno opravljal. Usposabljanje, ki poteka po vnaprej izdelanem programu, se mora zaključiti s preizkusom teoretične in praktične usposobljenosti za varno delo na delovnem mestu. Ali delodajalci zagotavljajo usposabljanje za varno delo, preverja inšpekcija nadzora varnosti in zdravja pri delu.

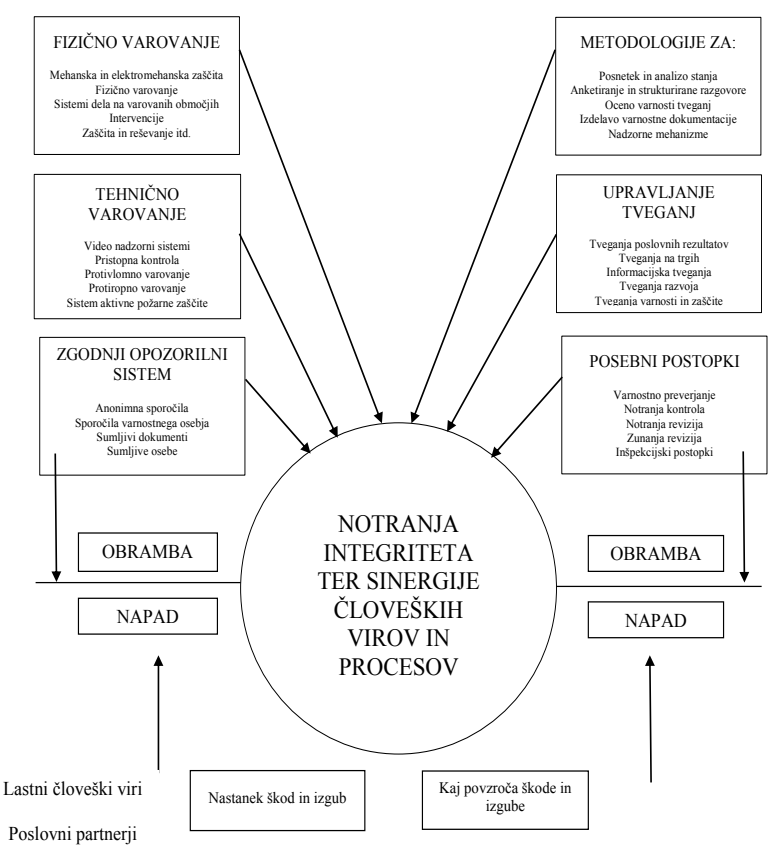
Posameznik in njegovo vedenje sta po navajanju Rančigajeve in Lobnikarja (2012) dva izmed ključnih dejavnikov tako pri zagotavljanju varnosti v podjetjih kot tudi pri informacijski varnosti organizacije. Uspeh ali neuspeh organizacije je v veliki meri odvisen od tega, kako posameznik opravi svoje delo ter od tega, kako samovarovalno pri tem deluje. Po navajanju Bernika in Prislanove (2016) morajo organizacije meriti tudi učinkovitost svoje informacijske varnosti, če želijo sprejeti pravilne odločitve in jih razviti v skladu z njihovimi varnostnimi potrebami. Merjenje informacijske varnosti organizacije pa je po njunem mnenju v praksi slabo razvito in zelo kompleksno. Rezultati študij kažejo, da je informacijska varnost odvisna od ukrepov za upravljanje informacijskih tveganj, zaposlenih in informacijskih virov, medtem ko imajo formalni in okoljski dejavniki manjši vpliv. Informacijska varnost se mora razvijati sistematično, kjer je po besedah Bernika in Prislanove (2016) priporočljivo, da začetni koraki vključujejo tehnične, logične in fizične varnostne kontrole, medtem ko najnaprednejše dejavnosti zadevajo pretežno strateške dejavnosti upravljanja.

3 INTEGRALNO ZAGOTAVLJANJE VARNOSTI V ORGANIZACIJI

Kako pomemben je za organizacijo korporativni varnostni menedžment, pove že njegova bistvena naloga, ki je obvladovanje varnostnih tveganj ter skrb za korporativno varnost. To so aktivnosti, ki prispevajo k varnosti organizacije ter preprečevanju notranjih ter zunanjih groženj.

3.1 Načrtovanje korporativne varnosti

Organizacije, ki si želijo poslovno preživeti ter biti uspešne, potrebujejo, po navajanju Kovačiča in Podvršiča (2014), za obvladovanje korporativnih varnostnih tveganj učinkovit varnostni menedžment. Brez varnostnega menedžmenta bi izjemno težko obvladovali notranja ter zunanja varnostna tveganja, ki jim grozijo. Za izdelavo varnostne politike organizacije je izrednega pomena, da izhajamo iz metodološke in vsebinske sheme pristopa k upravljanju korporativne varnosti. Le-ta nam daje celovit vpogled v nevarnosti, škodo in protiukrepe, kar je predstavljeno na sliki 1 (Vršec, 2014).



Slika 1: Metodološka in vsebinska shema pristopa k upravljanju korporativne varnosti (Vršec, 2014)

Korporativni varnostni menedžment se v organizacijah vedno pogosteje uveljavlja. Njegov bistveni cilj je izboljšanje učinkovitost poslovanja, preprečevanje prevar, ugleda in same zaščite organizacije. Kovačič in Podvršič (2014) navajata, da je končni cilj vsakega korporativnega varnostnega menedžerja dvig varnostne kulture pri zaposlenih. Bistveno je, da organizacije uvajajo nove strategije, tehnologije in metode za preprečevanje nevarnosti, ki jim pretijo, kajti v nasprotnem primeru imajo lahko težave v poslovanju oz. poslovne neuspehe.

3.1.1 Izdelava varnostnega načrta

V varnostnem načrtu so predstavljena dejstva sprejete varnostne politike organizacije in je pokazatelj varnostne strategije. Načrt je osnova oziroma podlaga za izdelavo notranjih aktov ter operativne varnostne dokumentacije, kot so: načrti varovanja, varnostni režimi, navodila itd. Varnostni načrt v osnovi zajema tri bistvene faze izvedbe, in sicer: posnetek obstoječega stanja; analizo obstoječega stanja in predloge varnostnih izboljšav, še posebej na strateškem nivoju.

Posnetek obstoječega stanja vključuje terenski pregled območij oziroma zgradb, preučitev varnostnih režimov, alarmnega in odzivnega sistema v sklopu upravljanja z VNC, proučitev organiziranosti sistema varovanja na strateškem ter operativnem nivoju, pregled varnostno vitalnih točk in obstoječih dokumentov varovanja (načrti varovanja, navodila itd.), razgovore s pooblaščenimi osebami, odgovornimi za posamezna področja varnosti ter zaščite, in ogled sistemov fizičnega ter tehničnega varovanja.

Analiza obstoječega stanja vsebuje nabor ter opis ranljivih varnostno vitalnih točk na območjih oziroma v zgradbah, predstavitev vsebine razgovorov s predstavniki poslovodstva in predstavitev vsebine razgovorov s pooblaščenimi osebami, odgovornimi za posamezna področja varnosti ter zaščite na strateškem nivoju, analizo ter povzetek (ugotovitev iz operativnega pregleda območij oziroma zgradb, ugotovitev v zvezi z vzpostavljenimi alarmnimi ter odzivnimi sistemi, ugotovitev iz ogleda sistema fizičnega in tehničnega varovanja, ugotovitev v zvezi z organiziranostjo sistema varovanja na strateškem nivoju, ugotovitev v zvezi z vzpostavljenimi varnostnimi režimi in ugotovitev iz pregleda obstoječih dokumentov varovanja) in analizo ranljivosti, varnostnih tveganj ter ogroženosti v notranjem in zunanjem okolju.

Predlogi varnostnih izboljšav morajo temeljiti na posnetku obstoječega stanja ter strokovni analizi ranljivosti, ogroženosti ter varnostnih tveganj v notranjem in zunanjem okolju, vzpostavitvi učinkovitega nadzora nad delovanjem sistema varovanja na strateškem ter operativnem nivoju, učinkovitega alarmnega ter odzivnega sistema v sklopu upravljanja VNC, sistema upravljanja z varnostnimi tveganji na strateškem nivoju, sistema neprekinjenega delovanja ter kriznega upravljanja korporativne varnosti v izrednih varnostnih razmerah, sistema notranje pravne ureditve na področju upravljanja z varnostno dokumentacijo, korporativnega varnostnega menedžmenta na strateškem ter operativnem nivoju in optimizaciji sinergije fizičnega ter tehničnega varovanja.

3.2 Preprečevanje škod, izgub in dvigovanje kulture organizacije

Načini varovanja organizacij se skozi obdobja razvijajo, spreminjajo ter prilagajajo glede na njihove lastne potrebe. Med prednosti tega razvoja in spreminjanja štejemo pretežno skrb za varnost, ki se prepušča organizacijam. Le-te imajo možnost, da v svoj varnostni sistem vključijo varnostne storitve zasebnih varnostnih podjetij ter s tem povečajo profesionalnost in zmanjšajo stroške zaščite. Da bi dosegli racionalne rešitve varnostnega sistema kot celote, je potreben pregled nad škodnimi pojavi ter izgubami kot tudi pregled nad stroški ter koristnostjo zaščitnih ukrepov. Zavarovalna politika se mora prilagajati trgu varnostnih storitev ter varnostnim interesom organizacij, kar vsebuje nova ter dodatna merila v zavarovalnih procesih. Varnost organizacije je interdisciplinarna ter celovita, postopoma se ustvarjajo politične ter strokovne možnosti za okrepitev ter uveljavitev nadzornih institucij, za dosego višje profesionalnosti, kar bi z vidika nudenja strokovne pomoči koristilo tudi organizacijam. Vršec (1993) tudi poudarja profesionalnost, optimalnost ter ekonomiko varnosti in nove oblike lastnine kot motiv za izboljšanje varnosti.

Organizacije, ki zanemarjajo pomen obvladovanja varnostnih tveganj, so na dolgi rok obsojene na stagnacijo oziroma na nerazvoj. Tveganja ter grožnje poslovnemu procesu dolgoročno in brez ustreznega obvladovanja v poslovanju prinesejo povečanje škodnih dogodkov, prekinitve poslovnih aktivnosti in povečanje tveganj, povezanih s kadrovskim potencialom, ali odtekanje ključnih poslovnih informacij. Vse to v celoti pripelje do zmanjšanja konkurenčne sposobnosti v zahtevnem globalnem okolju in izgubo ključnih poslovnih partnerjev ali strank (Čaleta, 2011). Ravno zato je pomembno, da lastniki organizacij pokažejo interes za čim boljšo zaščito premoženja, kapitala, procesov ter znanja in da menedžment, ki je odgovoren za zakonitost računovodskih izkazov ter drugih poslovnih listin, poskrbi za tak računovodski ter poslovni proces, da ne bo goljufiv in da varnostni menedžer skupaj z notranjo kontrolo ter pregledom poslovanja organizira oziroma ustvari tak opozorilni sistem, ki bo pravočasno odkril okoliščine za nastanek škodnih pojavov (Vršec, 1993).

3.3 Odgovornosti menedžerja

Menedžerji in lastniki organizacij se morajo oprijeti načel ter meril profesionalne etike upravljanja, vodenja, poslovanja ter odgovornosti. Osrednje načelo te etike je, da lastniki in menedžerji vsaj namerno ne spodbujajo ali delajo škode organizaciji. Če so menedžerji in lastniki zavestno usmerjeni k škodnim pojavom, je veliko možnosti, da bodo enaki tudi zaposleni. Vadnjal (2014) poudari, da je treba upoštevati, da ko je treba sprejeti težke odločitve, je najbolje, da se menedžerji in lastniki držijo svojih ključnih vrednot in s tem poskušajo objektivno in na pošten način pokazati skrb za družbo, organizacijo in celoten sistem.

Korporativni varnostni menedžer je pomemben in prav tako enakopraven partner pri vodenju ter upravljanju organizacije. Naloge ter odgovornosti korporativnega varnostnega menedžerja so po navajanju Gostiča (2014) soodgovornost za strateško odločanje ter upravljanje, upravljanje sprememb

v organizaciji na podlagi graditve zaupanja, varnostne kulture, močne socialne mreže, medsebojne povezanosti ter učenja in ne samo izvajanje korporativne varnosti kot podporni poslovni proces, zagotavljati tesno sodelovanje osnovnih ter podpornih poslovnih procesov v organizaciji, z namenom zagotavljanja varnosti premoženja, reda, zaščite ter neprekinjenega poslovanja, izvajanje dolžnostnega nadzorstva nad delom v organizaciji oziroma potekom osnovnih poslovnih procesov, prepričevati kolege in sodelavce znotraj organizacije, da je zagotavljanje varnosti sestavni del opravljanja njihovih del ter nalog in vsakodnevnih odločitev ter ne zgolj še eno delovno področje in upravljanje tveganj, izobraževanje s tega področja, vodenje delovnih skupin, načrtovanje ukrepov in drugo.

Menedžment in lastniki, ki dajo kaj na varnost organizacije, bodo poskrbeli za izobraženega, profesionalnega in prodornega varnostnega menedžerja za vodenje varnostne službe. Zavedati se morajo, kot meni Gostič (2014), da varnostni menedžer s svojim delom nedvomno pripomore k ohranjanju ter zviševanju vrednosti premoženja, ustvarjanju dobička za lastnike, izkazovanju integritete in družbene odgovornosti, pospeševanju prodaje izdelkov oziroma storitev ter s tem posledično ustvarjanju dobička, nemotenem delovanju vseh osnovnih ter podpornih procesov v družbi in samemu ogledu organizacije.

Glede na pomembnost korporativnega varnostnega menedžerja je izjemnega pomena, kam v strukturi organizacije ga umestimo. Izkušnje kažejo, da bi moral biti korporativni varnostni menedžer odgovoren direktno upravi organizacije oziroma samemu predsedniku uprave. Na ta način bi bil samostojen v koordinaciji varnostnih vprašanj in potreb ter neodvisen od ostalih služb znotraj organizacije. Podobno ugotavlja tudi Cavanagh (2005), ki postavlja korporativnega varnostnega menedžerja ob bok direktorja finančnega sektorja in ob bok direktorja informacijskega sektorja znotraj organizacije.

4 ZAKLJUČEK

Varnost je v sodobnem času nekaj samoumevnega. Življenja brez občutka varnosti si ne predstavljamo. Tako kot velja to za vsakega posameznika, je občutek varnosti in zaščite pomemben tudi v organizacijah. V dinamiki razvijajočega se 21. stoletja se morajo organizacije prilagajati in biti pripravljene na nevarnosti, kot so notranje ter zunanje grožnje organizacije. In ravno zaradi teh groženj stopa v ospredje preprečevanje škodnih pojavov in izgub ter vizija organizacije, da so varnostni mehanizmi tisti dejavniki, s katerimi lahko obvladujejo omenjene grožnje oziroma tveganja v organizaciji. Če preučimo dejansko stanje, se moramo zavedati, da bodo organizacije skoraj v celoti morale same poskrbeti za lastno zaščito, kar pomeni, da bodo morale same poiskati in zaposliti ustrezni kader, ki bo skrbel za varnost. To obliko varnosti definiramo kot korporativno varnost, ki pa v najširšem pomenu besede identificira in izvaja vse potrebne sistemske ukrepe za obvladovanje varnostnih tveganj v posamezni organizaciji. Integralna korporativna varnost ima prav tako pomembno vlogo pri blažitvi tveganj za nemoteno delovanje v organizacijah.

Področje integralne korporativne varnosti je v Sloveniji premalo obravnavana dejavnost, vendar izredno pomembna za pravilno delovanje celotnega sistema v

organizacijah. Lastniki oziroma direktorji organizacij morajo strmeti k temu, da zagotovijo in poskrbijo za potrebno varnost v organizaciji, zato je pomembno, da zaposlijo usposobljenega ter izkušenega varnostnega menedžerja z obravnavanega področja. Ta bo na podlagi izdelanega varnostnega načrta v organizaciji uvajal nove strategije in tehnologijo za preprečevanje nevarnosti, ki grozijo organizaciji. Vsaka organizacija mora zato imeti varnostni načrt, ki je osnovna podlaga za dokumente, ki so iz varnostnega vidika bistvenega pomena za organizacijo. Pri vseh nalogah, ki jih opravlja varnostni menedžer, pa ne smemo pozabiti na etično vlogo menedžerja, kar pomeni, da mora biti pošten in zaupanja vreden člen v organizaciji. Bistvo te etične vloge je, da ne spodbujajo ali delajo škode organizaciji (vsaj ne namerno), kajti če bodo menedžerji zavestno usmerjeni k škodnim pojavom, obstaja velika možnost, da bodo zaposleni delali enako, kar pa si ne želimo, saj je organizacija v takem primeru obsojena na stagnacijo in propad. Kot smo ugotovili, so za zagotavljanje celovite korporacijske varnosti ključnega pomena različni dejavniki, eden izmed njih je tudi uporaba različnih varnostnih standardov, ki omogočajo razvoj, proizvodnjo ter oskrbo proizvoda in s tem olajšajo medsebojno trgovino med državami ter jo naredijo pravno varno.

Zaključimo lahko, da je na področju integralne korporativne varnosti za razvoj potrebno še veliko truda. Strmeti moramo k temu, da bomo mlade motivirali in izobraževali na tem področju, saj bomo na ta način dosegli učinkovite premike v razvoju tega področja. Samemu razvoju pa bomo morali zagotoviti potreben čas, da se pokažejo morebitne napake, luknje v zakonih in praktični problemi pri izvajanju dejavnosti. S samim razvojem, odkrivanjem ter popravljanjem napak bomo zagotovili ustrezno varnost v organizacijah, kar pa nas bo privedlo do razvoja, uspešnosti in učinkovitosti organizacij, ki bodo posledično prinesle velik pečat k razvoju gospodarstva v Sloveniji.

Ne nazadnje pa, kot je zapisal tudi Houmann (2015), obstaja veliko dobrih razlogov, zakaj vzpostaviti varnostno oziroma korporativno varnostno politiko v organizaciji. A zavedati se moramo, da je treba začeti na začetku. Tako kot so Egipčani gradili piramide od spodaj navzgor, začnemo z varnostno politiko, definiramo cilje in nato gradimo korak za korakom. Na ta način in s premišljenimi koraki gradimo in ves čas izboljšujemo integralno korporativno varnost organizacije.

UPORABLJENI VIRI

Antončič, M. (2001). Nacionalni sistem varovanja tajnih podatkov. *Slovenska uprava, 1*(2), 28–29.

Bernik, I. in Prislan, K. (2016). Measuring information security performance with 10 by 10 model for holistic state evaluation. *PloS One, 11*(9), 1–33.

Brooks, D. J. in Corkill, J. (2014). Corporate security and the stratum of security management. V K. Walby in R. K. Lippert (ur.), *Corporate security in the 21st century* (str. 216–234). New York: Palgrave Macmillan.

Button, M. (2014). Foreword. V K. Walby in R. K. Lippert (ur.), *Corporate security in the 21st century* (str. VIII–IX). New York: Palgrave Macmillan.

Cavanagh, T. E. (2005). *Corporate security measures and practices.* New York: The Conference Board.

Cubbage, C. J. in Brooks, D. J. (2012). *Corporate security in the Asia-Pacific region: Crisis, crime, fraud, and misconduct*. Boca Raton: CRC Press.

Čaleta, D. (2011). Varnost mojega podjetja. *Podjetnik*, (Okt.), 40–41.

Čaleta, K. in Čaleta, D. (2013). Kadrovski management in krepitev varnostne kulture v korporacijskem okolju. *Korporativna varnost*, (3), 23–26.

Gerginova, T. (2016). Role of corporate security. V G. Meško in B. Lobnikar (ur.), *Criminal justice and security in Central and Eastern Europe: Safety, security, and social control in local communities: Conference proceedings* (str. 490–497). Ljubljana: Faculty of Criminal Justice and Security.

Gostič, Š. (2014). Odgovornost korporativno varnostnega menedžerja. *Korporativna varnost*, (8), 16–19.

Houmann, C. C. (18. 3. 2015). Corporate security policies: Their effect on security, and the real reason to have them. *The State of Security*. Pridobljeno na https://www.tripwire.com/state-of-security/security-awareness/corporate-security-policies-their-effect-security/

Kop, I. (1995). *Varovanje in zaščita poslovnih skrivnosti.* Ljubljana: Gospodarski vestnik.

Kovačič, A. in Podvršič, A. (2014). Korporativni varnostni management – nujnost sodobnih organizacij. *Korporativna varnost*, (7), 9–11.

Lalić, G. (2003). Varnostno preverjanje po zakonu o tajnih podatkih. *Pravna praksa, 22*(6/7), 20–22.

Lobnikar, B., Čaleta, D., Žaberl, M., Anžič, A. in Rančigaj, K. (2009). *Varnostna in organizacijska kultura v Slovenski vojski z vidika upravljanja s tajnimi podatki: Končno poročilo raziskovalne skupine Fakultete za varnostne vede*. Ljubljana: Fakulteta za varnostne vede.

Markelj, B. in Završnik, A. (2016). Kibernetska korporativna varnost mobilnih naprav: Zavedanje uporabnikov v Sloveniji. *Revija za kriminalistiko in kriminologijo, 67*(1), 44–60.

Modic, M., Lobnikar, B. in Dvojmoč, M. (2014). Policijska dejavnost v Sloveniji: Analiza procesov transformacije, pluralizacije in privatizacije. *Varstvoslovje, 16*(3), 217–241.

Predlog Zakona o kritični infrastrukturi. (2016). Pridobljeno na http://www.mo.gov.si/fileadmin/mo.gov.si/pageuploads/pdf/predpisi/obramba/v_pripravi/ZKI301216_predlog.doc

Rančigaj, K. in Lobnikar, B. (2012). Vedenjski vidiki zagotavljanja informacijske varnosti: pomen upravljanja informacijske varnostne kulture. V I. Bernik in G. Meško (ur.), *Informacijska varnost: Odgovori na sodobne izzive.* Pridobljeno na https://www.fvv.um.si/KonferencaIV/zbornik/Rancigaj_Lobnikar.pdf

Savski, S., Grilc, B., Jarc, S. in Mele, Z. (2012). *Zakon o detektivski dejavnosti (ZDD-1) s komentarjem – Zakon o zasebnem varovanju (ZZasV-1) s komentarjem.* Ljubljana: GV Založba.

Stare, J. (1995). Varovanje in zaščita poslovnih skrivnosti. V *Pravna država in uprava, II. srečanje upravnih delavcev Slovenije* (str. 107–118). Ljubljana: Visoka upravna šola.

Ustava Republike Slovenije. (1991). *Uradni list RS*, (33/91).

Vadnjal, J. (2014). Korporativna varnost in poslovna etika. *Korporativna varnost*, (6), 27–30.

Vedenik, L. in Miketić-Curman, S. (2013). Predlog standarda za integralno varnost kot temelj sistema vodenja in upravljanja varnostnega menedžmenta v organizacijah. V J. Taradi (ur.), *Menadžment i sigurnost, međunarodna znanstvena i stručna konferencija* (str. 447–454). Zagreb: Hrvatsko društvo inženjera sigurnosti.

Vršec, M. (1993). *Varnost podjetja – tokrat drugače.* Ljubljana: Viharnik.

Vršec, M. (2014). Strateško načrtovanje procesov korporativne varnosti. *Korporativna varnost,* (6), 23–26.

Walby, K. in Lippert, R. K. (2014). Introduction: Governing every person, place, and thing – critical studies of corporate security. V K. Walby in R. K. Lippert (ur.), *Corporate security in the 21st century* (str. 1–13). New York: Palgrave Macmillan.

Zakon o detektivski dejavnosti [ZDD]. (1994, 2002, 2005, 2007, 2010). *Uradni list RS*, (32/94, 96/02, 90/05, 60/07, 29/10).

Zakon o detektivski dejavnosti [ZDD-1]. (2011). *Uradni list RS*, (17/11).

Zakon o gospodarskih družbah [ZGD-1]. (2006, 2008, 2009, 2011, 2012, 2013, 2015, 2017). *Uradni list RS*, (42/06, 10/08, 68/08, 42/09, 33/11, 91/11, 32/12, 57/12, 82/13, 55/15, 15/17).

Zakon o industrijski lastnini [ZIL-1]. (2006, 2013). *Uradni list RS*, (51/06, 100/13).

Zakon o podjetjih [ZPod]. (1988, 1989, 1990). *Uradni list SFRJ*, (77/88, 40/89, 61/90).

Zakon o tajnih podatkih [ZTP]. (2001, 2003, 2006, 2010, 2011). *Uradni list RS*, (87/01, 135/03, 50/06, 9/10, 60/11).

Zakon o varnosti in zdravju pri delu [ZVZD-1]. (2011). *Uradni list RS*, (43/11).

Zakon o varstvu osebnih podatkov [ZVOP-1]. (2007). *Uradni list RS*, (94/07).

Zakon o zasebnem varovanju [ZZasV]. (2003, 2007). *Uradni list RS*, (126/03, 16/07).

Zakon o zasebnem varovanju [ZZasV-1]. (2011). *Uradni list RS*, (17/11).

Zakon o zasebnem varovanju in obveznem organiziranju službe varovanja [ZZVO]. (1994, 1997). *Uradni list RS*, (32/94, 23/97).

O avtorju:

Dr. Miha Dvojmoč, predavatelj na Fakulteti za varnostne vede Univerze v Mariboru. E-pošta: miha.dvojmoc@fvv.uni-mb.si