
Vloga korporativne varnosti na ministrstvih v Republiki Sloveniji

VARSTVOSLOVJE
leto 2025
letn. 27
str. 1–20

Karmen Černigoj, Miha Dvojmoč

Namen prispevka:

Namen prispevka je predstaviti temeljito analizo koncepta korporativne varnosti, njeno opredelitev in vlogo ter preučiti pravno ureditev in procese, ki zagotavljajo varnost na ministrstvih v Republiki Sloveniji.

Metode:

Na podlagi analize pisnih virov smo pripravili celovit pregled relevantne literature in zakonskih aktov, ključnih za obravnavano tematiko. Raziskovalno delo temelji na kvantitativnem pristopu, izvedenem s spletnim anketiranjem zaposlenih na ministrstvih.

Ugotovitve:

Ugotovljena je bila pomembna povezava med udeležbo v programih varnostnega usposabljanja in izvajanjem pravnih procesov korporativne varnosti. Vendar pa ni bila ugotovljena povezava med zaznano zadostnostjo varnostnih ukrepov za zaščito pred sodobnimi grožnjami in vrsto delovnega mesta zaposlenih na posameznem ministrstvu, prav tako ni bila ugotovljena povezava med hitrostjo in učinkovitostjo odziva na varnostne incidente ter mandatom zaposlenih. Rezultati razkrivajo pomanjkanje pozornosti na področju zagotavljanja varnosti »know-howa« in zaščite intelektualne lastnine ter kažejo na potrebo po dodatnih izboljšavah na področju integritete in vodenja v upravi.

Omejitve /uporabnost raziskave:

Omejitev raziskave nam predstavlja vprašljivost glede iskrenosti odgovorov anketirancev. Poleg tega se je med izvajanjem ankete izkazalo, da med uslužbenci ministrstev ni bilo enotnega razumevanja pojma in sestavin korporativne varnosti, kar lahko vpliva na zanesljivost in interpretacijo zbranih podatkov. Raziskava lahko služi kot orodje za izboljšanje varnostne kulture in integriranje korporativne varnosti na ministrstvih.

Praktična uporabnost:

Prispevek ponuja poglobljen pregled celovitega zakonskega okvira korporativne varnosti na ministrstvih ter predstavlja ugotovitve in rezultate, ki služijo kot temelj za prihodnje raziskave.

Izvirnost/pomembnost prispevka:

Obravnavanje korporativne varnosti na ministrstvih je namenjeno strokovnjakom s področja korporativne varnosti in javnim uslužbencem, ki si prizadevajo zagotoviti celovito in učinkovito varnost javnega sektorja. S prispevkom želimo raziskovalce spodbuditi k nadaljnji obravnavi te tematike.

Ključne besede: korporativna varnost, javna uprava, ministrstva, Slovenija

UDK: 005.934:354(497.4)

The role of corporate security at ministries in the Republic of Slovenia

Purpose:

The aim of this paper is to present a thorough analysis of the concept of corporate security, its definition and role, and to examine the legal framework and processes that ensure security in ministries in the Republic of Slovenia.

Design/Methods/Approach:

Based on an analysis of written sources, we have prepared a comprehensive review of the relevant literature and legal acts key to the topic at hand. The research work is based on a quantitative approach, carried out through an online survey of ministry staff.

Findings:

A significant correlation was found between participation in security training programmes and the implementation of corporate security legal processes. However, no correlation was found between the perceived sufficiency of security measures to protect against co-occurring threats and the type of job held by employees in each ministry, nor was there a correlation between the speed and effectiveness of response to security incidents and the tenure of employees. The results reveal a lack of attention to ensuring the security of know-how and the protection of intellectual property, and point to the need for further improvements in the area of integrity and governance in the administration.

Research Limitations /Implications:

A limitation of the survey is the question of the sincerity of the respondents' answers. In addition, during the course of the survey, it became apparent that there was no common understanding of the concept and components of corporate security among ministry staff, which may affect the reliability and interpretation of the data collected. The survey can be used as a tool to improve the security culture and integrate corporate security in ministries.

Practical Implication:

The paper provides an in-depth overview of the comprehensive legal framework for corporate security in ministries and presents findings and results

that serve as a basis for future research.

Originality/Value:

Addressing corporate security in ministries is aimed at corporate security professionals and civil servants working to ensure the comprehensive and effective security of the public sector. This paper aims to encourage researchers to further address this topic.

Keywords: corporate security, public administration, ministries, Slovenia

UDC: 005.934:354(497.4)

1 UVOD

V današnjem dinamičnem svetu, kjer se informacijska tehnologija nenehno razvija in globalizacija pospešuje tok informacij, postaja korporativna varnost na ministrstvih ključni element za učinkovito delovanje javnega sektorja. Ministrstva, kot ključni sestavni del kritične infrastrukture, morajo imeti vzpostavljene učinkovite varnostne mehanizme, saj lahko vsaka motnja ali napad ogrozi delovanje države in posledično nacionalno varnost (Szczepaniuk idr., 2020). Zaradi vse večjih tveganj, tako znotraj kot zunaj organizacij, je nujno vzpostaviti celovit sistem korporativne varnosti. Notranja tveganja, kot so človeške napake, je mogoče ublažiti z rednim izobraževanjem in ozaveščanjem zaposlenih o varnostnih protokolih (Szczepaniuk idr., 2020). Na drugi strani pa se v povezavi z zunanjimi tveganji vse pogostejše pojavljajo digitalni napadi, pri katerih kibernetiski vdori ogrožajo zaupnost podatkov in delovanje informacijskih sistemov ministrstev (Ministrstvo za zunanje in evropske zadeve, 2023).

Temelj korporativne varnosti predstavljajo kakovostne pravne in varnostne smernice, ki urejajo zaščito občutljivih podatkov, preprečevanje nepooblaščenega dostopa in varnostnih kršitev. Z integracijo pravnih, varnostnih in zakonskih ukrepov lahko ministrstva učinkovito zaščitijo svoje operacije, sredstva in osebe. Zakonodajni okvir, kot so »Zakon o tajnih podatkih (ZTP)« (2001), »Zakon o varstvu osebnih podatkov (ZVOP-2)« (2022), »Zakon o javnih uslužbencih (ZJU)« (2002), »Zakon o informacijski varnosti (ZInfV)« (2018) itd., natančneje opredeljuje pravila glede dostopa in varstva podatkov, pomembnih za preprečevanje varnostnih tveganj (Oyewole idr., 2023).

Za uspešno soočanje s temi izzivi je izjemno pomembno, da se vzpostavi celovit pristop h korporativni varnosti in se dosledno upoštevajo procesi korporativne varnosti, ki so ključni za zagotavljanje celovite varnosti v javnem sektorju. Ti procesi so razdeljeni v šest temeljnih kategorij, med katerimi so zagotavljanje zakonitega in nemotenega delovanja, varovanje varnostnega »know-howa«, zaščita tehnologij in informacijskih sistemov, varstvo stvarnopравnih in intelektualnih pravic, zagotavljanje zasebne varnosti ter skrb za varno delovno okolje (Dvojmoč, 2020).

2 OPREDELITEV KORPORATIVNE VARNOSTI

Korporativna varnost obsega celovit sklop strategij, politik, postopkov in tehnologij, ki jih organizacija implementira za zaščito svojega osebja, fizične lastnine, digitalnih sredstev in informacij pred notranjimi in zunanji grožnjami. Njen osnovni cilj je prepoznavanje, ocenjevanje in zmanjševanje tveganj, s čimer se zagotavlja neprekinjeno poslovanje (Security Executive Council, n. d.). Za uspešno izvedbo neprekinjenega poslovanja je ključno tesno sodelovanje med različnimi oddelki (informacijska tehnologija, kadrovska, pravna, operativna itd.), kar omogoča pravočasno zaznavanje in preprečevanje potencialnih groženj. Večina organizacij za izvajanje teh nalog vzpostavi poseben varnostni oddelk (Dvojmoč, 2017). Vršec in Vršec (2023) poudarjata, da zakon sicer ne zahteva oblikovanja posebne službe za korporativno varnost, vendar določa imenovanje odgovornih oseb, ki morajo sodelovati z drugimi upravljavci in nosilci kritične infrastrukture. To predstavlja osnovo za vzpostavitev enote, ki strateško upravlja varnostna tveganja in zagotavlja uravnotežen razvoj posameznih področij varnosti.

Pravna in regulatorna podlaga, ki jo tvorijo statut, pravilniki in notranji akti, je temelj vsakega celovitega varnostnega programa (Dvojmoč, 2020). Ta dokumentacija določa osnovne varnostne koncepte in smernice ter ureja postopke za zaščito premoženja, varstvo pri delu, požarno varstvo, ekološke vidike in industrijsko lastnino. Učinkovito strateško načrtovanje zahteva jasno opredeljene procese, kot so varovanje podatkov, zaščita poslovnih skrivnosti, integrirano fizično in tehnično varovanje ter varnost elektronskih komunikacij. Ključna načela dobre korporativne uprave vključujejo ločitev odgovornosti, jasna pooblastila in ukrepe za preprečevanje korupcije (Vršec, 2014).

Za organizacije v Evropski uniji je izjemno pomembno, da njihovi notranji pravilniki upoštevajo stroge evropske regulative. Medtem ko se uredbe in sklepi uporabljajo neposredno v vseh državah članicah od dneva njihove uveljavitve, morajo države članice direktive prenesti v svojo nacionalno zakonodajo v določenem roku. Uporaba standardov sicer ni obvezna, vendar organizacijam omogoča, da dokažejo skladnost s predpisi, kar poleg pravne usklajenosti prispeva tudi k boljši učinkovitosti in zmanjševanju tveganj. Skladnost s standardi povečuje ugled in zaupanje v organizacijo, tako pri poslovnih partnerjih kot pri strankah, kar posledično krepi njeno konkurenčnost in poveča zaupanje deležnikov (European Commission, n. d.; Vršec, 2014). Standardi so mednarodno dogovorjene smernice, ki jih oblikujejo strokovnjaki z različnih področij z namenom vzpostavitve najboljših praks. Opisujejo najučinkovitejše, varne in preverjene načine za izvedbo postopkov, izdelavo izdelkov ali izvajanje storitev. Njihov glavni cilj je zagotoviti kakovost, varnost, skladnost z zakonodajo, zmanjševanje tveganj ter spodbujanje trajnostnega razvoja in inovacij. Standardi se uporabljajo v številnih sektorjih, med drugim na področjih zdravja in zdravstvenih storitev, informacijskih tehnologij, upravljanja in storitev, varnosti ter obvladovanja tveganj. Pomembni so tudi v prometu, energetiki, gradbeništvu, inženirstvu ter na področjih, kot so raznolikost in vključevanje, okoljska trajnost, prehrana in kmetijstvo ter materiali (ISO, International Organization for Standardization, n. d.). Zaradi svoje široke uporabnosti standardi predstavljajo temelj za usklajeno delovanje različnih

akterjev na trgu, omogočajo primerljivost med sistemi in povečujejo zaupanje javnosti v varnost in kakovost izdelkov ter storitev.

Za dolgoročni uspeh organizacij je nepogrešljivo stalno prilagajanje in izboljševanje varnostnih sistemov. Pri tem ima osrednjo vlogo kombinacija pravnih, tehničnih in organizacijskih ukrepov. Redno spremljanje tveganj, revizij varnostnih postopkov in usposabljanje zaposlenih so nepogrešljivi elementi, ki omogočajo pravočasno odzivanje na spremembe v varnostnem okolju. Celovit pristop h korporativni varnosti omogoča organizacijam učinkovito zaščito pred sodobnimi grožnjami in ohranjanje konkurenčnosti na trgu. Sistematičen pristop in integracija varnostnih politik v vse operativne procese zagotavljata visoko raven zaščite in zanesljivosti (Dvojmoč, 2017).

Pomembno je razlikovati med korporativno in institucionalno varnostjo, čeprav obe področji ščitita ljudi in sredstva. Institucionalna varnost je usmerjena v zaščito javnih institucij, pri čemer je poudarek na ohranjanju varnosti, reda in stabilnosti, skladno s strožimi vladnimi predpisi. Korporativna varnost pa temelji na industrijskih standardih in zakonodaji, specifični za zasebni ali javni sektor. V praksi številne organizacije kombinirajo oba pristopa, saj uporabljajo institucionalne protokole za javno varnost ter korporativne strategije za notranje obvladovanje tveganj (»Institutional security personnel«, n. d.; Verstein, 2017)

Korporativna varnost ni izključno značilna samo za zasebni sektor, temveč tudi javni sektor. Izraz »korporativna varnost« se ohranja tudi v kontekstu ministrstev in državnih organov, saj se osredotoča na funkcionalni in operativni pristop, ki temelji na obvladovanju tveganj. Operativni elementi, kot so ocena tveganj, zaščita sredstev in obvladovanje groženj, so univerzalni in prisotni v vseh sektorjih. Korporativna varnost je tesno povezana s korporativno identiteto, kar predstavlja njeno edinstveno značilnost, ki je ne najdemo pri drugih oblikah varnosti (Lalić idr., 2019).

3 MINISTRSTVA V REPUBLIKI SLOVENIJI

Ministrstva imajo pomembno vlogo v državni upravi in so ključni del izvršilne veje oblasti, saj so odgovorna za izvajanje upravnih nalog v Republiki Sloveniji. Njihovo delovanje temelji na ustavi, zakonih in drugih podzakonskih predpisih (»Zakon o državni upravi (ZDU-1)«, 2002). Organizacija državne uprave sledi sektorskim, funkcionalnim in teritorialnim načelom, zato je vsako ministrstvo ustanovljeno za upravljanje in opravljanje upravnih nalog na enem ali več določenih področjih (Tičar, 2019).

Ena temeljnih zahtev v državni upravi je ohranjanje politične nevtralnosti in nepristranskosti. Ta standard velja za ministrstva in njihove javne uslužbenke, saj zagotavlja, da se ohranjata pravičnost in objektivnost ter da noben posameznik, pravna oseba ali interesna skupina ni neupravičeno favorizirana (»ZDU-1«, 2002). Pomembno je poudariti, da funkcionarji v državnih in lokalnih organih, vključno z ministri in državnimi sekretarji, ne spadajo v kategorijo javnih uslužbencev v tradicionalnem smislu, saj opravljajo svojo funkcijo le za čas trajanja ali do prenehanja mandata.

Vsako ministrstvo vodi minister, ki ministrstvo zastopa in sprejema odločitve v skladu s sprejetimi politikami, zakoni in drugimi regulativnimi akti. Kadar se sooča z zapletenimi upravnimi ali strokovnimi vprašanji, je minister pooblaščen, da skliče strokovni svet, če je ta ustanovljen. Poleg ministra ima vsako ministrstvo tudi državnega sekretarja, ki pomaga pri izvajanju dodeljenih nalog in lahko deluje v imenu ministra v času njegove odsotnosti, vendar brez glasovalne pravice na sejah vlade (»ZDU-1«, 2002).

Notranja organizacija ministrstva je razdeljena na tri glavne enote: kabinet, direktorat in sekretariat. Kabinet, ki ga vodi njegov vodja, je ključen za upravljanje strokovnih, organizacijskih in upravnih odgovornosti ministra. Direktorat, pod vodstvom generalnega direktorja, vključuje urade, sektorje, službe in oddelke. Sekretariat, ki ga vodi generalni sekretar, skrbi za odnose z javnostmi, protokolarne zadeve, finančno poslovanje in načrtovanje. Te enote sodelujejo pri zagotavljanju nemotenega usklajevanja in učinkovitega delovanja ministrstva. Poleg tega se lahko po potrebi ustanovijo dodatne službe za podporo ministrski funkciji (Tičar, 2019).

V Sloveniji je upravni okvir razdeljen med 19 ministrstev, od katerih je vsako pristojno na različnih področjih državne uprave, pri čemer je vsako pristojno za določeno področje delovanja, ki je jasno opredeljeno v zakonodaji (»ZDU-1«, 2002). V nadaljevanju so predstavljene pristojnosti izbranih ministrstev.

Ministrstvo za delo, družino, socialne zadeve in enake možnosti ureja delovna razmerja ter pravice zaposlenih in delodajalcev. Skrbi za zaposlovanje, brezposelnost, čezmejno delo in zaposlovanje tujcev. Prizadeva si za preprečevanje dela in zaposlovanja na črno ter zagotavlja socialno varstvo invalidom, mladini, otrokom in družinam. Poleg tega spodbuja enake možnosti za oba spola in vključevanje invalidov v družbo (»ZDU-1«, 2002; Prevec, 2024).

Ministrstvo za digitalno preobrazbo upravlja informacijsko-komunikacijske sisteme ter skrbi za digitalizacijo javne uprave. V njegovi pristojnosti potekajo zbiranje in analiza podatkov, razvoj digitalnih kompetenc in zagotavljanje elektronskih storitev, vključno z varnimi elektronskimi interakcijami (Rebolj, 2024).

Ministrstvo za finance nadzira javne finance, makroekonomsko stabilnost in davčno politiko. Ukvarja se s preprečevanjem pranja denarja, organizacijo iger na srečo ter upravljanjem državnega proračuna in dolga. Ključna naloga ministrstva je tudi zagotavljanje stabilnosti finančnega sistema (Ministrstvo za finance, 2024).

Ministrstvo za gospodarstvo, turizem in šport spodbuja gospodarski razvoj, internacionalizacijo podjetij, tehnološke inovacije ter trajnostno gospodarstvo. Poleg tega skrbi za razvoj turizma in športne infrastrukture ter regulacijo notranjega trga (»ZDU-1«, 2002).

Ministrstvo za kmetijstvo, gozdarstvo in prehrano skrbi za razvoj podeželja, varnost in kakovost hrane, kmetijsko politiko ter gozdarske in ribiške dejavnosti. Njegove pristojnosti vključujejo tudi veterinarstvo in zaščito rastlin (»ZDU-1«, 2002).

Ministrstvo za kulturo ureja področja kulturne dediščine, umetnosti, medijev in slovenskega jezika. Spodbuja kulturno ustvarjalnost in varovanje kulturnih spomenikov ter skrbi za pluralnost medijskega prostora (»ZDU-1«, 2002).

Ministrstvo za kohezijo in regionalni razvoj upravlja evropska kohezijska sredstva ter spodbuja enakomeren regionalni razvoj. Skrbi za usklajevanje nacionalnih politik s strateškimi dokumenti Evropske unije (Ministrstvo za kohezijo in regionalni razvoj, 2024).

Ministrstvo za notranje zadeve zagotavlja javni red, vodi policijo ter upravlja migracijsko politiko in izdajo osebnih dokumentov. Nadzira volilne postopke in varnost javnih zborovanj ter ureja registracijo društev in političnih strank (Ministrstvo za notranje zadeve, 2024).

Ministrstvo za javno upravo skrbi za delovanje javnega sektorja, vključno z zaposlovanjem v javni upravi, sistemom javnih naročil in dostopom do informacij javnega značaja. Poleg tega ureja delovanje nevladnih organizacij in lokalne samouprave (»ZDU-1«, 2002).

Ministrstvo za obrambo skrbi za obrambno varnost in zaščito pred naravnimi nesrečami. Upravljajo ga tudi sistemi civilne zaščite, vojaška varnost in pomoč vojnim veteranom (»ZDU-1«, 2002).

Ministrstvo za pravosodje ureja organizacijo in delovanje sodnega sistema, državnega tožilstva in notariata. Skrbi za izvrševanje kazenskih sankcij ter varstvo človekovih pravic in pravnih interesov države (»ZDU-1«, 2002).

Ministrstvo za infrastrukturo načrtuje razvoj prometne infrastrukture, vključno z železniškim, pomorskim, zračnim in cestnim prometom. Njegova naloga je izboljšanje prometne povezanosti in varnosti (Ministrstvo za infrastrukturo, 2024).

Ministrstvo za naravne vire in prostor skrbi za varstvo okolja, upravljanje vodnih virov ter geodetske dejavnosti. Prav tako nadzira področje jedrske varnosti in varstva pred ionizirajočimi sevanji (»ZDU-1«, 2002).

Ministrstvo za okolje, podnebje in energijo se osredotoča na trajnostno rabo energije, podnebne spremembe in ravnanje z odpadki. Sprejema zakonodajo na področju energetike in varstva okolja ter nadzira ravnanje z radioaktivnimi odpadki (Ministrstvo za okolje, podnebje in energijo, 2024).

Ministrstvo za solidarno prihodnost se ukvarja s socialno stanovanjsko politiko, dolgotrajno oskrbo in deinstitucionalizacijo starejših. Njegova naloga je preprečevanje stanovanjskih stisk ter izboljšanje dostopnosti do neprofitnih stanovanj (Prevec, 2024).

Ministrstvo za visoko šolstvo, znanost in inovacije spodbuja razvoj visokega šolstva, znanstvenih raziskav in inovacij. Zavzema se za akademsko avtonomijo in financiranje raziskovalne dejavnosti (Hvala, 2024).

Ministrstvo za vzgojo in izobraževanje ureja predšolsko, osnovno in srednje šolstvo ter izobraževanje odraslih. Njegova naloga je zagotavljanje kakovostnega in dostopnega izobraževalnega sistema (Ministrstvo za vzgojo in izobraževanje, 2024).

Ministrstvo za zdravje upravlja zdravstveni sistem, javno zdravje in zdravstveno varstvo. Njegove naloge obsegajo nadzor nad zdravstvenim zavarovanjem, kemijsko varnostjo in prehransko varnostjo (»ZDU-1«, 2002).

Ministrstvo za zunanje in evropske zadeve zastopa Slovenijo v mednarodnih odnosih, sodeluje v mednarodnih organizacijah ter skrbi za zaščito interesov slovenskih državljanov v tujini (»ZDU-1«, 2002).

4 ZAGOTAVLJANJE PRAVNE UREDITVE IN PROCESOV KORPORATIVNE VARNOSTI NA MINISTRSTVIH

Po obravnavi širšega pojma korporativne varnosti se osredotočamo na njeno pomembno podkategorijo, integralno korporativno varnost. Sheshukova in Teimurova (2021) jo opisujeta kot celovit sistem varnosti organizacije, ki mu omogoča stabilnost, razvoj in odpornost na različne grožnje. Integralna korporativna varnost je stanje podjetja, ki omogoča njegovo preživetje in razvoj, ter sistem upravljanja, ki zagotavlja celovito zaščito interesov organizacije in drugih subjektov pred vsemi oblikami groženj. Vršec (2012) opisuje integralno korporativno varnost kot preplet vseh ključnih varnostnih področij v družbi. Sem sodijo varstvo pred naravnimi in drugimi nesrečami, zaščita pred industrijskimi nesrečami, požarna varnost, varstvo okolja, zaščita in reševanje, varnost in zdravje pri delu ter varovanje osebnih in tajnih podatkov. Poleg tega vključuje tudi varovanje informacijskih sistemov, intelektualne lastnine in poslovnih skrivnosti, skrb za arhive, fizično in tehnično varovanje ljudi in premoženja ter zaščito ugleda in konkurenčnih prednosti.

Korporativna varnost predstavlja v okviru ministrstev celostni pristop k zaščiti javnih uslužbencev, zunanjih sodelavcev ter obiskovalcev, pa tudi fizičnih sredstev, prostorov in informacij pred notranjimi in zunanjimi grožnjami. Njen ključni namen je pravočasno prepoznati, oceniti in učinkovito obvladovati tveganja, s čimer se zagotavlja varno in neprekinjeno delovanje državnih organov (Dvojmoč, 2020; Security Executive Council, n. d.). Tovrsten pristop zahteva tudi vzpostavitev trdnega pravnega okvira, ki določa postopke in standarde za zagotavljanje varnosti. Ta okvir vključuje številne pravne procese, kot so upravljanje tveganj, fizična, tehnična in informacijska varnost, zagotavljanje neprekinjenega poslovanja, krizno upravljanje, zaščita ključnih informacij, varnost zaposlenih ter varstvo pri delu (ICS, Institut za korporativne varnostne študije, n. d.). V nadaljevanju bomo podrobneje obravnavali šest pravnih procesov korporativne varnosti, s katerimi se organizacijam zagotavlja sprejemanje tveganja na obvladljivo raven. Procesi so večplastni in vključujejo naslednje ključne vidike (Dvojmoč, 2017; Dvojmoč, 2020):

- zagotavljanje zakonitega in nemotenega delovanja;
- zagotavljanje varnostnega »know-how«;
- zaščita tehnologij in informacijskega sistema;
- zaščita stvarnopравnih pravic in pravic intelektualne lastnine;
- zagotavljanje zasebne varnosti;
- zagotavljanje varnega delovnega mesta.

Ti procesi so med seboj povezani in tvorijo celostni varnostni sistem, ki omogoča, da ministrstva lahko učinkovito obvladujejo tako notranja kot zunanja tveganja (Dvojmoč, 2017).

4.1 Zakonito in nemoteno delovanje

Za zagotovitev skladnega in učinkovitega delovanja poslovnih dejavnosti je nujna vzpostavitev notranjega pravnega okvira. Okvir mora vključevati celovito obravnavo različnih kritičnih vidikov, vključno z ureditvijo varnostnih vprašanj,

varovanjem poslovnih skrivnosti, izvajanjem protikorupcijskih mehanizmov in zagotavljanjem integritete zaposlenih, s čimer varujejo organizacijske interese (Dvojmoč, 2020).

Temelj vsakega varnostnega sistema je zagotavljanje zakonitega in nemotenega delovanja. Ta proces zajema izvajanje notranjih politik, pravilnikov in direktiv, ki so v skladu z veljavno zakonodajo. Ministrstva sprejemajo lastne notranje akte, s katerimi zagotavljajo, da se zakonski nameni prenesejo v praktične ukrepe, ki urejajo vsakodnevno delovanje. Tako se zagotovi, da ministrstva delujejo brez nepotrebnih motenj, kar je bistveno za nemoteno izvajanje nalog v javnem interesu (»ZDU-1«, 2002; Dvojmoč, 2020). Zagotavljanje zakonitega in nemotenega delovanja organizacije temelji na vzpostavitvi jasnih notranjih pravil in direktiv, ki so skladni z nacionalno zakonodajo. »ZDU-1« (2002) določa, da morajo ministrstva delovati v skladu s predpisi Evropske unije in pravnimi akti Republike Slovenije. Zato so notranje uredbe, pravilniki in navodila ključni za prenos zakonskih določb v vsakodnevne praktične ukrepe (»ZDU-1«, 2002). Spoštovanje teh določb in urejanje pravic javnih uslužbencev ureja Zakon o javnih uslužbencih. Ta določa pravice, dolžnosti in načela, ki se pričakujejo od javnih uslužbencev ter dolžnosti organa do uslužbenca (»ZJU«, 2002). Za učinkovito upravljanje je nujno, da se notranji akti in smernice na posameznih ministrstvih redno posodablajo. S tem se zagotovi enoten sistem delovanja, ki omogoča hitro odzivanje na morebitne kršitve ali varnostne incidente. Poseben poudarek je tudi na preprečevanju korupcije in zagotavljanju integritete javnih uslužbencev, kar je urejeno z »Zakonom o integriteti in preprečevanju korupcije (ZIntPK)« (2011). S tem se zmanjšuje tveganje za motnje v delovanju in zagotavlja visoka stopnja nadzora nad izvajanjem nalog. Varnostni postopki, povezani z zakonitostjo poslovanja, so zato ključnega pomena za stabilnost in zanesljivost državnih institucij.

4.2 Zagotavljanje varnostnega »know-howa«

Pravno zagotavljanje varnostnega »know-howa«, prilagojenega organizaciji, vključuje več ključnih komponent, ki so bistvene za zaščito njegovih interesov. To zajema temeljite preiskave in odkrivanje domnevnih nezakonitih dejanj v organizaciji, odpravljanje dejavnosti, namenjenih prevaram ali goljufiji ter izvajanje proaktivnih ukrepov z obveščevalno in protiobveščevalno dejavnostjo za zaščito organizacije (Dvojmoč, 2020).

Ministrstvo za javno upravo ima ključno vlogo pri nadzoru izvajanja predpisov, ki urejajo upravno poslovanje, kot jih določajo »ZDU-1« (2002) in »Zakon o splošnem upravnem postopku (ZUP)« (2006) ter »Uredba o upravnem poslovanju« (2018). Upravni inšpektorji, opredeljeni v Zakonu o inšpekcijskem nadzoru, imajo pooblastila za pregledovanje zaupnih dokumentov in izvajanje nadzora nad zagotavljanjem skladnosti, kar omogoča odkrivanje kršitev in sprejemanje ustreznih ukrepov (»Zakon o inšpekcijskem nadzoru (ZIN)«, 2007). »Zakon o integriteti in preprečevanju korupcije (ZIntPK)« (2011) zavezuje javne uslužbence na ministrstvu k preprečevanju in odpravljanju korupcije. Izvajanje teh nalog ni odgovornost le javnih uslužbencev, temveč tudi Komisije

za preprečevanje korupcije. Slednja je odgovorna za nadzor, preiskovanje in odkrivanje korupcije ter stremi k spoštovanju integritete (»ZIntPK«, 2011). Boj proti finančni kriminaliteti vzpostavlja »Zakon o preprečevanju pranja denarja in financiranja terorizma (ZPPDFT-2)« (2022), v skladu s katerim izvajajo inšpekcijski nadzor številni pristojni organi, kot so Banka Slovenije, Agencija za trg vrednostnih papirjev, Agencija za zavarovalni nadzor, Finančna uprava Republike Slovenije, Tržni inšpektorat Republike Slovenije, Agencija za javni nadzor nad revidiranjem, Odvetniška zbornica Slovenije in Notarska zbornica Slovenije ter Policija. Pomembno je poudariti, da zakon obravnava tudi vprašanji zaupnosti in tajnih podatkov, katerih temeljni okvir na tem področju predstavljata »Zakon o tajnih podatkih (ZTP)« (2001) in »Uredba o varnostnem preverjanju in izdaji dovoljenj za dostop do tajnih podatkov« (2021). Organi in agencije, ki sodelujejo pri odobritvi in nadzoru dostopa do tajnih podatkov so Ministrstvo za obrambo – Obveščevalna varnostna služba (OVS), Slovenska obveščevalna varnostna agencija (SOVA) in Ministrstvo za notranje zadeve – Direktorat za policijo in druge varnostne naloge. Inšpektorat za notranje zadeve in Inšpektorat za obrambo izvajata nadzore nad spoštovanjem predpisov o določanju, označevanju, varovanju in dostopu do tajnih podatkov. Ugotovitve posredujejo Uradu Vlade Republike Slovenije za varovanje tajnih podatkov, ki nadzira celoten sistem ravnanja s tajnimi podatki ter spremlja skladnost z varnostnimi standardi in opravlja strokovne naloge na tem področju. Tovrstno sodelovanje je ključnega pomena za delovanje ministrstev na področju obveščevalne dejavnosti, s poudarkom na protiobveščevalni dejavnosti (Britovšek in Čretnik, 2016; »ZTP«, 2001).

4.3 Zaščita tehnologij in informacijskega sistema

Pravna zaščita tehnologij in informacijskega sistema zajema ukrepe za zagotavljanje organizacijske in tehnične informacijske varnosti, kar vključuje pripravo in sprejem notranjih politik in aktov. Ti okviri ne zajemajo le oblikovanja in sprejetja ustreznih notranjih politik, temveč tudi neprekinjen nadzor ter ocenjevanje njihovega učinkovitega izvajanja (Dvojmoč, 2020).

Ministrstva morajo skladno z zakonskimi določili določiti notranjo politiko in postopke za obvladovanje tveganj ter zagotoviti varnost informacijskih sistemov. To vključuje analizo tveganj, politiko neprekinjenega poslovanja, načrte obnovitve in odziva ter varnostne ukrepe, razdeljene na organizacijske, logično-tehnične in tehnične kategorije. Organizacijski ukrepi zajemajo vzpostavitev varnostnih politik, določitev notranje organizacije delovnih mest, imenovanje odgovornih oseb ter izobraževanje zaposlenih na področju varnosti. Logično-tehnični ukrepi vključujejo uporabo naprednih varnostnih tehnologij, kot so klasifikacija podatkov, požarni zidovi in sistemi za zaznavanje vdorov, ki zagotavljajo zaščito informacijskih sistemov. Tehnični ukrepi pa obsegajo fizično varovanje informacijskih tehnologij, vključno z mehanskimi zaščitnimi napravami, sistemi za nadzor dostopa in postopki pregleda oseb (»ZInfV«, 2018; Karanikas in Zerguine, 2024). »ZInfV« (2018) prav tako pooblašča inšpektorje za nadzor nad skladnostjo in varovanjem informacijskih sistemov ministrstev. Ta ureditev omogoča standardizacijo varnostnih procesov v vseh ministrstvih in prispeva k

večji odpornosti državnega sektorja pred sodobnimi tveganji ter krepitvi zaupanja javnosti. S tem pristopom se dosega visoka učinkovitost zaščite tehnologij in informacijskih sistemov.

4.4 Zaščita stvarnopravnih pravic in pravic intelektualne lastnine

Na področju pravne zaščite stvarnopravnih pravic in pravic intelektualne lastnine zakonodaja ureja zaščito lastninske pravice in druge stvarne pravice organizacije, v kar se vključujejo patenti, blagovne znamke, modeli in njihovo poreklo. Prav tako imajo avtorske pravice tudi organizacije, ki ščitijo izvirna avtorska dela, bistvena za zaščito pred krajo oz. ponarejanjem (Dvojmoč, 2020).

Pravni postopki na tem področju vključujejo registracijo patentov, blagovnih znamk in modelov, pa tudi urejanje avtorskih pravic. Zagotavljanje ustreznega pravnega varstva omogoča, da se morebitne kršitve in zlorabe hitro zaznajo in sankcionirajo, s čimer se ohranja integriteta in konkurenčnost ministrstev. Ta sistematični pristop je ključen za zaščito intelektualne lastnine in zagotavljanje, da se inovacije in ustvarjalnost negujejo in spodbujajo v javnem sektorju. »Stvarnopravni zakonik (SPZ)« (2002) določa temeljna načela stvarnega prava in ureja posest ter stvarne pravice, vključno z njihovim pridobivanjem, prenosom, varstvom in prenehanjem, s čimer vzpostavlja jasen pravni okvir za upravljanje stvarnega premoženja. »Zakon o industrijski lastnini (ZIL-1)« (2006) natančno določa pravice industrijske lastnine, kot so patenti, modeli, znamke in geografske označbe, ter ureja postopke njihove registracije, podelitve, razveljavitve in sodnega varstva, kar zagotavlja celovito pravno zaščito teh. »Zakon o avtorski in sorodnih pravicah (ZASP)« (2007) pa vzpostavlja pravni okvir za zaščito avtorskih del in sorodnih pravic, opredeljuje postopke licenciranja ter določa pravila za varstvo intelektualnih stvaritev, med katere sodijo književna, glasbena, vizualna in avdiovizualna dela, kar je ključno za zagotavljanje pravne varnosti avtorjev in uporabnikov avtorskih del. Pravna ureditev na tem področju ministrstvom omogoča, da s pravnimi sredstvi ukrepajo proti morebitnim kršitvam in zagotovijo, da so njihovi intelektualni viri zaščiteni pred nepooblaščenim razširjanjem ali krajo.

4.5 Zagotavljanje zasebne varnosti

Pravni okvir, ki ureja področje zasebne varnosti, vključuje ključne segmente, ki so bistveni za varovanje premoženja. Okvir določa zakonske podlage in prakse, ki zagotavljajo varovanje zasebnega premoženja ter vzpostavljajo mehanizme za nadzor nad zunanjimi in notranjimi grožnjami. Ključnega pomena je pravočasno prepoznavanje, spremljanje in zmanjševanje morebitnih tveganj, kar se dosega s celovitim varnostnim načrtovanjem (Dvojmoč, 2020).

Pomemben del sistema varovanja predstavlja tudi zaščita kritične infrastrukture, ki je eden izmed temeljev nacionalne varnosti. Gre za objekte in sisteme, katerih delovanje je ključno za stabilnost države. Slovenski pravni red to področje ureja s pomočjo več ključnih predpisov, med katerimi ima osrednjo vlogo »Zakon o zasebnem varovanju (ZZasV-1)« (2011), ki krovno določa pogoje, način in organizacijo zasebnega varovanja.

Dopolnjuje ga »Zakon o kritični infrastrukturi (ZKI)« (2017), ki opredeljuje kritično infrastrukturo kot objekte, ki so bistvenega pomena za državo, kjer bi njihova motnja ali nedelovanje lahko povzročila resne posledice za nacionalno varnost, gospodarstvo, vitalne družbene funkcije, zdravje, varnost in splošno blaginjo. Lastništvo in upravljanje kritičnih infrastruktur imajo tudi ministrstva, in sicer jih upravljajo glede na delovno področje pristojnega ministrstva (»ZKI«, 2017). Uredba o obveznem organiziranju varovanja in Zakon o zasebnem varovanju (ZZasV-1) dopolnjujeta ta okvir, saj urejata organizacijo in izvajanje varnostnih ukrepov, pri čemer se varnostne storitve zagotavljajo preko postopka javnega naročanja (Dvojmoč idr., 2019). Varovanje kritične infrastrukture zahteva tudi medsebojno sodelovanje s pristojnimi službami, kot so policija, regijski center za obveščanje, gasilci in drugi, kar omogoča učinkovito odzivanje v primeru varnostnih incidentov. Ključna sestavina celovitega varovanja je dokumentiran hierarhični pristop k načrtovanju varnosti, ki vključuje oceno stopnje tveganja, omogoča zavezancem učinkovito upravljanje in obvladovanje potencialnih groženj. Ključni elementi ocene stopnje tveganja zajemajo podatke o zavezancu, opis varovanega območja, analizo ranljivosti, analizo ogroženosti, analizo tveganj ter celovito oceno stopnje tveganja, vključno z verjetnostjo nastanka posledic (»Uredba o obveznem organiziranju varovanja«, 2012).

V skladu z uredbo Policija varuje varovane osebe in objekte glede na pomembnost ter stopnjo ogroženosti po hierarhičnem pristopu ter na tretji stopnji varuje ministra in objekte, v katerih je sedež ministrstva, in sicer Ministrstvo za zunanje in evropske zadeve, Ministrstvo za obrambo in Ministrstvo za notranje zadeve. Policija lahko varuje tudi druge funkcionarje in pomembne tuje osebe, če je njihovo življenje zaradi opravljanja funkcije resno ogroženo. Varovanje se uvede na predlog ministra ali predstojnika organa in temelji na oceni ogroženosti. Po potrebi se lahko varujejo tudi družinski člani, policija pa varovanje tujih oseb določi glede na funkcijo in lastno presojo ter ga lahko tudi zavrne (»Uredba o varovanju določenih oseb, prostorov, objektov in okolišev objektov, ki jih varuje policija«, 2013).

4.6 Zagotavljanje varnega delovnega mesta

Zagotavljanje pravne varnosti na delovnem mestu zajema pravna ureditev varovanja oseb in osebnih podatkov, pri čemer so zajeti tako notranji zaposleni kot zunanji sodelavci in obiskovalci. Pravne zahteve morajo obsegati varstvo okolja ter ukrepe za zagotavljanje varnosti in zdravja pri delu, s ciljem preprečevanja nesreč, bolezni in ustvarjanja varnega delovnega okolja (Dvojmoč, 2020).

Skladno z »Zakonom o varstvu osebnih podatkov (ZVOP-2)« (2022) in »Splošno uredbo o varstvu podatkov (GDPR)« (2016) se osebni podatki opredeljujejo kot vse informacije, ki omogočajo identifikacijo posameznika. Ta zakonodaja zagotavlja celovit in natančen okvir za obdelavo podatkov v javnem in zasebnem sektorju, pri čemer mora biti vsak poseg v zasebnost utemeljen in zakonit. Z uveljavljanjem strogih smernic in zaščitnih ukrepov ne ščiti le pravic posameznikov, temveč tudi spodbuja zaupanje in integriteto obdelave podatkov na ministrstvih (»ZVOP-2«, 2022; »GDPR«, 2016). Hkrati »Zakon o varstvu okolja (ZVO-2)« (2022) določa

13 temeljnih načel za trajnostno varstvo okolja, vključno z zmanjšanjem emisij, učinkovitim ravnanjem z odpadki, proaktivni ukrepi za preprečevanje večjih nesreč in izključevanje nevarnih snovi iz proizvodnih procesov. Ministrstva so z zakonskimi določbami zavezana vzpostaviti in doslednemu izvajanju teh ukrepov ter ozaveščati javnost o okolijski tematiki (»ZVO-2«, 2022). Ministrstvo je dolžno izvajati celovite ukrepe za zagotavljanje varnosti in zdravja pri delu. Te izvaja s preprečevanjem in odpravljanjem nevarnosti pri delu, obveščanjem in usposabljanjem delavcev ter zagotavljanjem ustrezne organiziranosti. Delavci oz. javni uslužbenci na ministrstvih imajo opredeljene pravice in dolžnosti v zvezi z varnostjo in zdravjem pri delu. Ta dvojna obveznost zagotavlja, da se varnostni protokoli dosledno uporabljajo na vseh področjih, kar zagotavljajo ministrstva z imenovanjem enega ali več strokovnih delavcev za opravljanje strokovnih nalog v zvezi z varnostjo in zdravjem pri delu (»Zakon o varnosti in zdravju pri delu (ZVZD-1)«, 2011).

5 RAZISKAVA KORPORATIVNE VARNOSTI NA MINISTRSTVIH V REPUBLIKI SLOVENIJI

Namen raziskave, ki je bila izvedena s spletnim anektiranjem, je zagotoviti celovito razumevanje dinamike korporativne varnosti na ministrstvih v Sloveniji. Uporabljen vzorec snežne kepe je povečal udeležbo, a hkrati povzročil pristranskost, saj ni predstavljal celotne populacije. Skupaj je sodelovalo 219 relevantnih deležnikov, ki so zastopali različne kategorije delovnih mest. 70 % je zasedalo uradniška delovna mesta, 28 % strokovno-tehnična delovna mesta in 2 % druga delovna mesta. Od tega je 65 % žensk, 30 % moških in 5 % posameznikov, ki so se identificirali kot drugo. Povprečna delovna doba 13,93 leta kaže na dolgoletno institucionalno predanost.

Korporativno varnost sestavlja šest pravnih procesov, med katerimi se na ministrstvu daje največji poudarek zaščiti tehnologij in informacijskega sistema z 78,4 % ($\chi = 3,92$), sledita zagotavljanje zakonitega in nemotenega poslovanja s 75,4 % ($\chi = 3,77$) ter zagotavljanje varnega delovnega mesta s 70,4 % ($\chi = 3,52$). Nekoliko manj poudarka se daje zagotavljanju zasebne varnosti s 66,6 % ($\chi = 3,33$), zaščiti stvarnopravnih pravic in pravic intelektualne lastnine s 63,0 % ($\chi = 3,15$) ter najmanj zagotavljanju varnosti »know-howa« z 59,2 % ($\chi = 2,96$) (tabela 5.1).

$n = 219$	1	2	3	4	5
	Zelo nizek poudarek				Zelo visok poudarek
Zagotavljanje zakonitega in nemotenega poslovanja.	4 %	8 %	26 %	28 %	33 %
Zagotavljanje varnosti »know-howa«.	15 %	17 %	36 %	20 %	12 %
Zaščita tehnologij in informacijskega sistema.	3 %	7 %	23 %	31 %	36 %
Zaščita stvarnopravnih pravic in pravic intelektualne lastnine.	10 %	19 %	34 %	21 %	16 %
Zagotavljanje zasebne varnosti.	7 %	14 %	34 %	30 %	15 %
Zagotavljanje varnega delovnega mesta.	5 %	11 %	31 %	31 %	21 %

Tabela 5.1: Poznavanje pravnih procesov korporativne varnosti

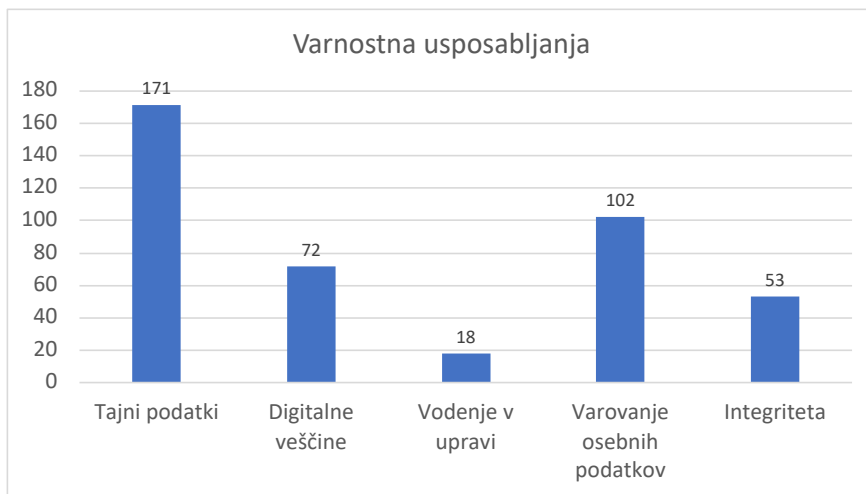
Ker smo želeli združiti pravne procese korporativne varnosti v eno spremenljivko, smo uporabili faktorsko analizo. Rezultati kažejo, da lahko s skupnimi faktorji pojasnimo 82,1 % celotne variance in s prvim faktorjem pojasnimo 57,7 % variance merjenih spremenljivk, kar predstavlja kritičen konstrukt, ki upravičuje nadaljnje preiskave. S Cronbachovim koeficientom alfa smo izračunali zelo visoko zanesljivost za faktor naklonjenosti pravnim procesom korporativne varnosti, kar se je potrdilo pri uteževanju na faktorjih. Spremenljivke imajo zelo veliko utež le na enem faktorju, kar nam zagotavlja, da je vseh šest procesov naklonjenih novi spremenljivki. S slednjo smo ustvarili novo spremenljivko – naklonjenost pravnim procesom korporativne varnosti (tabela 5.2).

Tabela 5.2:
Naklonjenost pravnim procesom korporativne varnosti

	<i>KMO</i>	<i>Variance</i>	<i>α</i>
Naklonjenost pravnim procesom korporativne varnosti	0,821	57,74 %	0,890

Anketiranci so ocenili, da se izobraževanj o varnosti udeležujejo občasno, s povprečno oceno 2,97 ($SD = 1,31$) na Likertovi lestvici, kar kaže na zmerno pogostost udeležbe. Graf 5.1 prikazuje, da so najpogostejše obiskana izobraževanja na področju tajnih podatkov, varovanja osebnih podatkov in digitalnih veščin. Opazno nižja udeležba usposabljanj je bila na področju integritete in vodenja v upravi. 12 % anketirancev se je usposabljal še na drugih področjih, kot so varstvo pri delu, varni na internetu, lažne novice, hibridne grožnje, digitalna varnost, kibernetska varnost, varstvo pred požarom in obrambno načrtovanje.

Graf 5.1:
Varnostna usposabljanja



S Spearmanovim koeficientom korelacije smo preverili povezanost med spremenljivkama naklonjenost pravnim procesom korporativne varnosti in pogostost udeleževanj izobraževanj o varnosti na ministrstvu (tabela 5.3). S 5-% tveganjem lahko trdimo, da med udeleževanjem usposabljanj in pravnimi procesi korporativne varnosti obstaja povezanost. Rezultati kažejo na pozitivno korelacijo, kar pomeni, da večja, kot je udeležba na varnostnih usposabljanjih, večja je naklonjenost pravnim procesom korporativne varnosti. To prispeva k večji

ozaveščenosti in pozitivnemu odnosu do izvajanja ključnih pravnih procesov korporativne varnosti, kar je bistveno za krepitev celovite varnosti ministrstev.

	<i>R</i>	<i>p</i>
Spearmanov koeficient korelacije	0,292	0,001

Tabela 5.3:
Povezanost
poznavanja
pravnih procesov
korporativne varnosti
in udeležbe na
usposabljanjih

Anketiranci so s povprečno oceno 3,22 ($SD = 0,95$) ocenili, da ministrstva zadostno izvajajo varnostne ukrepe. S povprečno oceno 3,59 ($SD = 0,98$) pa so ocenili ustreznost varnostnih ukrepov pred sodobnimi tveganji. Ta ocena nakazuje, da velik del zaposlenih meni, da trenutni varnostni protokoli niso niti zelo učinkoviti niti neučinkoviti, temveč zmerno zadostni za zaščito pred sodobnimi tveganji. Poleg splošne ocene so anketiranci izpostavili številna kritična področja, na katerih je treba dodatno okrepiti varnostne ukrepe. Večina je poudarila pomen okrepitve ukrepov na področju korporativne varnosti, varovanja podatkov, dostopa do skupnih map, paradoksa, varnostne kulture, osebnih in drugih podatkov, zaščite elektronskih naprav, informacijske varnosti, terorističnih tveganj, varnosti zaposlenih pred naravnimi nesrečami, večjega zavedanja zaposlenih o pomenu varnosti na posameznih področjih, legitimacije oseb/preverjanja oseb ob prihodu na ministrstvo, sabotaž, kibernetičnih napadov, zlorabe podatkov, človeških virov, odnosa do socialnih omrežij, fizičnega varovanja, etike zaposlenih, mobinga, zunanjih izvajalcev, integritete, zdravstvenega varstva, protibevšečevalne dejavnosti, hibridnih groženj, področja izobraževanja zaposlenih ter številnih drugih področij. Vsa omenjena področja so bila poudarjena kot kritične točke, ki zahtevajo močnejše zaščitne strategije za zagotovitev organizacijske varnosti pred sodobnimi grožnjami.

Tabela 5.4 prikazuje rezultate z enostavno analizo variance (ANOVA), kjer smo preverili, ali obstaja razlika v ocenjevanju zadostnosti varnostnih ukrepov glede na tip delovnega mesta (strokovno-tehnično v primerjavi z uradniškimi delovnimi mesti), ter ugotovili, da s 5-% tveganjem ne moremo trditi, da obstaja razlika med vrednotenjem zadostnosti varnostnih ukrepov ministrstva, zaščito pred sodobnimi grožnjami in delovnim mestom. Ta ugotovitev kaže, da so trenutni varnostni protokoli enotno dojemani, ne glede na sistemizacijo delovnega mesta, kar bi lahko bila posledica standardiziranih postopkov in skupnega varnostnega okvira, ki ga uporabljajo vsa ministrstva.

	<i>df</i>	<i>F</i>	<i>p</i>
ANOVA	1	0,038	0,845

Tabela 5.4:
Povezanost med
zadostnostjo
varnostnih
ukrepov in
delovnim mestom

V zadnjih treh mesecih se je zaznalo povprečno 31,8 % varnostnih tveganj, med katerimi je največ zaznanih s področja informacijskih tveganj (72 %), tveganj človeških virov (18 %), zlorabe podatkov (18 %), naravnih in drugih nesreč (7 %), kriminalnih tveganj (6 %) in kategorija drugo (18 %). Medtem je 18 % anketirancev poročalo o nezakonitem lobiranju in pomanjkljivosti definiranja, katere informacije niso javnega značaja, drugi pa v zadnjih treh mesecih niso odkrili nobenih dodatnih tveganj poleg zgoraj navedenih.

Pri vprašanju, ki je ocenjevalo hitrost in učinkovitost odzivov na morebitne varnostne incidente znotraj ministrstev, so anketiranci ocenili, da je njihovo ministrstvo obravnavalo te incidente hitro in učinkovito. Podatki so razkrili

povprečno oceno 3,59 ($SD = 0,98$) na Likertovi lestvici, kar kaže, da se zaposleni na različnih ministrstvih strinjajo, da njihove institucije izkazujejo zadovoljivo stopnjo ažurnosti in učinkovitosti pri obvladovanju varnostnih groženj.

Dabi ugotovili, ali obstaja kakršna koli povezava med hitrostjo in učinkovitostjo odziva na varnostne incidente ter delovno dobo zaposlenih na ministrstvih, smo izračunali Pearsonov korelacijski koeficient (tabela 5.5). Rezultati kažejo, da med tema spremenljivkama ni pomembne povezave. Natančneje povedano, s 95-% gotovostjo lahko trdimo, da ne obstaja povezanost med hitrim in učinkovitim odzivom na morebitne varnostne incidente ter delovno dobo zaposlenih na ministrstvih. Z drugimi besedami, delovna doba zaposlenih na ministrstvih ne vpliva na zaznano hitrost in učinkovitost odziva na varnostne incidente.

Tabela 5.5:
Povezanost
med
varnostnimi
incidenti in
delovno dobo

	<i>R</i>	<i>p</i>
Pearsonov koeficient korelacije	-0,016	0,839

6 ZAKLJUČEK IN RAZPRAVA

Korporativna varnost na ministrstvih v Republiki Sloveniji predstavlja ključno področje, ki pomembno prispeva k splošni varnosti in stabilnosti delovanja teh institucij. Rezultati raziskave so pokazali, da nekatera področja še vedno zahtevajo dodatno pozornost in nadaljnje izboljšave.

Pozitivna povezava med redno udeležbo na varnostnih usposabljanjih in boljšim poznavanjem pravnih procesov korporativne varnosti jasno poudarja pomembnost vlaganja v izobraževanje zaposlenih, kar posledično vodi v dvig varnostne kulture. Kljub temu pozitivnemu rezultatu so bile ugotovljene določene vrzeli, zlasti na področju zaščite varnostnega »know-howa« in intelektualne lastnine, kar lahko pripišemo zaupni in tajnostni naravi delovanja protiobveščevalnih dejavnosti znotraj ministrstev. Zaskrbljujoče je dejstvo, da je bilo najmanj udeležbe na usposabljanjih o integriteti in vodenju v javni upravi. To jasno kaže na potrebo po večji spodbudi in širšem naboru izobraževalnih programov ter ozaveščanju zaposlenih na omenjenih področjih.

Raziskava je pokazala, da se varnostni ukrepi izvajajo na enoten način, ne glede na vrsto delovnega mesta ali delovno dobo zaposlenih na ministrstvih. To dokazuje, da imajo ministrstva že vnaprej določene postopke in ukrepe, ki zagotavljajo enoten pristop k varnosti v celotni organizaciji. Kljub temu pa ti ukrepi zahtevajo nenehno nadgrajevanje in prilagajanje novim varnostnim tveganjem, ki jih prinašajo sodobni izzivi. Le s proaktivnim in celovitim pristopom lahko ministrstva učinkovito preprečujejo varnostne incidente ter zagotavljajo hiter in učinkovit odziv ob morebitnih kršitvah, kar je bistveno za nemoteno delovanje.

Pomembno je izpostaviti, da so na te rezultate lahko vplivale različne omejitve, ki lahko vplivajo na zanesljivost zaključkov. Poleg pomislekov glede iskrenosti anketirancev je bila ob zaključku ankete ugotovljena še ena omejitev. Med glavnimi omejitvami je pomanjkanje celovitega razumevanja koncepta korporativne varnosti med zaposlenimi na ministrstvih. Nezadostno predhodno izobraževanje in usposabljanje ter nezmožnost popolnega razumevanja anketnih vprašanj ogrožata natančnost zbranih podatkov. Zaradi navedenih omejitev

so lahko odgovori deloma pristranski, kar poudarja potrebo po dodatnem usposabljanju, jasnih razlagah temeljev korporativne varnosti ter zagotavljanju zmanjšanja pristranskosti raziskovalnega okolja v prihodnjih raziskavah. Tako bi izboljšali zanesljivost raziskovalnih rezultatov, kar bi pripomoglo k večji objektivnosti in verodostojnosti raziskovalnih podatkov.

Kot je bilo že poudarjeno, v sistemu korporativne varnosti na ministrstvih obstajajo vrzeli, ki jih je treba odpraviti. Ključni korak k izboljšanju varnosti je zagotovitev ustreznega usposobljenega kadra, kar ne pomeni zgolj imenovanja odgovorne osebe, temveč tudi vzpostavitev notranjega oddelka ali službe za korporativno varnost. Pri tem je smiselno upoštevati primere dobrih praks, kjer so službe za korporativno varnost že integrirane v organizacijsko strukturo in tesno sodelujejo z drugimi službami znotraj organizacije (npr. UKC Ljubljana: Služba za korporativno varnost, Telekom Slovenije: Center kibernetске varnosti in odpornosti itd.). Kot poudarja Kandžič (2024), sicer razpolagamo z ustreznim znanjem, vendar je pomanjkanje usposobljenega kadra eden ključnih izzivov. To dodatno potrjuje potrebo po večjem poudarku korporativne varnosti znotraj ministrstev, kar ne zahteva le naložbe v izobraževanje in usposabljanje, temveč tudi ponovno oceno in posodobitev obstoječih sistemizacij delovnih mest ter oblikovanje novih delovnih mest, namenjenih izvajanju korporativne varnosti.

Integracija korporativne varnosti v procese ministrstev bi omogočala celovito razumevanje delovanja organizacije in njenih ranljivosti, kar je ključno za učinkovito upravljanje varnostnih tveganj. Ob tem je treba upoštevati, da tehnološke in organizacijske inovacije neprestano prinašajo nova tveganja. Medtem ko je bil nekoč glavni izziv digitalizacija, danes predstavlja izziv umetna inteligenca, ki v javnem in zasebnem sektorju odpira nova varnostna vprašanja in tveganja. Zato je nujno, da ministrstva zagotovijo usposobljen notranji kader, ki bo sposoben prepoznavanja in obvladovanja prihodnjih tveganj ter prilagajanja nenehno spreminjajočemu se varnostnemu okolju.

Ostaja pa vprašanje, v kolikšni meri Slovenija pri razvoju sistemov korporativne varnosti sledi evropskim smernicam in najboljšim praksam. Primerjalna analiza z državami, kot sta Nizozemska in Finska, bi omogočila boljše oceno stanja in primerljivosti slovenskih pristopov s standardi v Evropski uniji.

Za nadaljnje raziskave bi radi spodbudili raziskavo na področju korporativne varnosti glede na posamično ministrstvo, ob tem pa predlagamo uporabo alternativnih metod vzorčenja, ki bi omogočile širšo reprezentativnost in povečale natančnost raziskovalnih izsledkov. V Sloveniji imamo 19 ministrstev, od katerih ima vsako svojo pristojnost dela ter s tem tudi svoj nabor varnostnih tveganj in ranljivosti, značilnih za njegovo področje delovanja. Takšen pristop bi omogočil natančnejše razumevanje njihovih varnostnih potreb in posledično prispeval k celovitemu razumevanju in optimizaciji varnostnega okvira na ministrstvih.

UPORABLJENI VIRI

Britovšek, J. in Čretnik, A. (2016). Obveščevalno-varnostni sistem Republike Slovenije: reorganizacija in sistemske rešitve. *Varstvoslovje: revija za teorijo in prakso varstvoslovja*, 18(3), 325–348.

- Dvojmoč, M. (2020). *Integralna korporativna varnost* [Študijsko gradivo]. Fakulteta za varnostne vede.
- Dvojmoč, M. (2017). Integralna korporativna varnost. *Varstvoslovje: revija za teorijo in prakso varstvoslovja*, 19(3), 252–272. https://www.fvv.um.si/rV/arhiv/2017-3/04_Dvojmoc_rV_2017-3.pdf
- Dvojmoč, M., Beković, M., Mandelj, G., Sotlar, A., Vačovnik, M., Babnik, A. in Prešljlić, M. (2019). *Zagotavljanje in naročanje zasebne varnosti v Republiki Sloveniji: Priročnik za naročnike in ponudnike storitev zasebnega varovanja v Republiki Sloveniji*. Univerzitetna založba Univerze v Mariboru.
- European Commission. (n. d.). *European standards*. https://single-market-economy.ec.europa.eu/single-market/european-standards_en
- Hvala, D. (18. 3. 2024). *Obrazložitev zaključnega računa za leto 2023*. Ministrstvo za visoko šolstvo, znanost in inovacije.
- Institutional security personnel. (n. d.). V *Law Insider*. <https://www.lawinsider.com/dictionary/institutional-security-personnel>
- ISO, International Organization for Standardization. (n. d.). *ISO: Global standards for trusted goods and services*. <https://www.iso.org/home.html>
- Kandžič, A. (2024). Dinamični varnostni izzivi Republike Slovenije. *Korporativna varnost*, 24(34), 10–14. <https://www.ics-institut.si/assets/uploads/revija/34/34-stevilka-revije-Korporativna-varnost.pdf>
- Karanikas, N. in Zerguine, H. (2024). Are the new safety paradigms (only) about safety and sufficient to ensure it? An overview and critical commentary. *Safety Science*, 170, 106367. <https://doi.org/10.1016/j.ssci.2023.106367>
- ICS, Institut za korporativne varnostne študije. (n. d.). *Korporativna varnost*. <https://www.ics-institut.si/korporativna-varnost>
- Lalić, V., Čeranić, P. in Sikimić, M. (2019). Private and/or corporate security: Are there conceptual similarities and differences? *Journal of security and criminal sciences* 1(1), 51–65.
- Ministrstvo za finance RS. (2024). *Poslovno poročilo Ministrstva za finance za leto 2023*.
- Ministrstvo za infrastrukturo RS. (2024). *Poslovno poročilo Ministrstva za infrastrukturo za leto 2023*.
- Ministrstvo za kohezijo in regionalni razvoj RS. (2024). *Poslovno poročilo za leto 2023*.
- Ministrstvo za notranje zadeve RS. (2024). *Zaključni račun 2023*.
- Ministrstvo za okolje, podnebje in energijo RS. (2024). *Poslovno poročilo Ministrstva za okolje, podnebje in energijo*.
- Ministrstvo za vzgojo in izobraževanje RS. (2024). *Obrazložitev zaključnega računa za leto 2023*.
- Ministrstvo za zunanje in evropske zadeve. (12. 4. 2023). *Odziv Ministrstva za zunanje in evropske zadeve na kibernetški napad*. <https://www.gov.si/novice/2023-04-12-odziv-ministrstva-za-zunanje-in-evropske-zadeve-na-kibernetски-napad/>
- Oyewole, O. O., Fakeyede, O. G., Okeleke, E. C., Apeh, A. J. in Adaramodu, O. R. (2023). Security considerations and guidelines for augmented reality implementation in corporate environments. *Computer Science and IT Research*

- Journal*, 4(2), 69–84. <https://doi.org/10.51594/csitrj.v4i2.607>
- Prevec, N. (18. 3. 2024). *Obrazložitev zaključnega računa za leto 2023*. Ministrstvo za delo, družino, socialne zadeve in enake možnosti.
- Rebolj, M. (15. 3. 2024). *Obrazložitev zaključnega računa za leto 2023*. Ministrstvo za digitalno preobrazbo.
- Security Executive Council. (n. d.). *What Is Corporate Security?* <https://securityexecutivecouncil.com/insight/corporate-security-career/what-is-corporate-security-2097>
- Sheshukova, T. G. in Teimurova, A. R. (2021). Integrated corporate security: The definition, key constituents. *National Interests: Priorities and Security*, 17(2), 274–295.
- Stvarnopravni zakonik (SPZ). (2002, 2013, 2020). *Uradni list RS*, (87/02, 91/13, 23/20).
- Szczepaniuk, E. K., Szczepaniuk, H., Rokicki, T. in Klepacki, B. (2020). Information security assessment in public administration. *Computers & Security*, 90, 101709. <https://doi.org/10.1016/j.cose.2019.101709>
- Tičar, B. (2019). *Uvod v razumevanje upravnega prava in javne uprave*. Univerzitetna založba Univerze v Mariboru.
- Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov). (2016). *Uradni list Evropske unije*, L 119, 1–88.
- Uredba o obveznem organiziranju varovanja. (2012). *Uradni list RS*, (80/12).
- Uredba o upravnem poslovanju. (2018, 2020, 2021, 2022, 2023, 2024). *Uradni list RS*, (9/18, 14/20, 167/20, 172/21, 68/22, 89/22, 135/22, 77/23, 24/24).
- Uredba o varovanju določenih oseb, prostorov, objektov in okolišev objektov, ki jih varuje policija. (2013, 2020, 2022). *Uradni list RS*, (63/13, 23/20, 144/20, 102/22).
- Uredba o varnostnem preverjanju in izdaji dovoljenj za dostop do tajnih podatkov. (2021). *Uradni list RS*, (4/21).
- Verstein, A. (2017). The corporate governance of national security. *Washington University Law Review*, 95, 775.
- Vršec, M. in Vršec, M. (2023). Pomembnost službe za korporativno varnost pri upravljalcih kritične infrastrukture in izvajalcih bistvenih storitev. *Korporativna varnost*, 23(33), 34–36. <https://www.ics-institut.si/assets/uploads/revija/33-%C5%A1tevilka/33-stevilka-revije-Korporativna-varnost.pdf>
- Vršec, M. (2014). Strateško načrtovanje procesov korporativne varnosti. *Korporativna varnost*, 14(6), 23–26. https://www.ics-institut.si/assets/uploads/revija/6-%C5%A1tevilka/06_KV_marec_2014_internet_LoRes.pdf
- Vršec, M. (2012). Vloga korporativne varnosti. *Korporativna varnost*, 12(1), 9–11. https://www.ics-institut.si/assets/uploads/revija/1-%C5%A1tevilka/01_KV_september-2012_Internet_LoRes.pdf
- Zakon o avtorski in sorodnih pravicah (ZASP). (2007, 2008, 2013, 2015, 2016, 2019, 2022). *Uradni list RS*, (16/07, 68/08, 110/13, 56/15, 63/16, 59/19, 130/22).
- Zakon o državni upravi (ZDU-1). (2002, 2005, 2007, 2009, 2010, 2012, 2013, 2014, 2016, 2021, 2022, 2023). *Uradni list RS*, (52/02, 113/05, 89/07, 126/07, 48/09, 8/10, 8/12, 21/12, 47/13, 12/14, 90/14, 51/16, 36/21, 82/21, 189/21, 153/22, 18/23).

Zakon o industrijski lastnini (ZIL-1). (2006, 2013, 2020, 2023). *Uradni list RS*, (51/06, 100/13, 23/20, 76/23).

Zakon o informacijski varnosti (ZInfV). (2018, 2021, 2022, 2023). *Uradni list RS*, (30/18, 95/21, 130/22, 18/, 49/23).

Zakon o inšpekcijskem nadzoru (ZIN). (2007, 2014). *Uradni list RS*, (43/07, 40/14).

Zakon o integriteti in preprečevanju korupcije (ZIntPK). (2011, 2020, 2022, 2023). *Uradni list RS*, (69/11, 158/20, 3/22, 16/23).

Zakon o javnih uslužbencih (ZJU). (2002, 2007, 2008, 2012, 2012, 2020, 2021, 2022). *Uradni list RS*, (56/02, 63/07, 65/08, 69/08, 69/08, 40/12, 158/20, 203/20, 202/21, 3/22).

Zakon o kritični infrastrukturi (ZKI). (2017, 2021). *Uradni list RS*, (75/17, 189/21).

Zakon o obrambi (ZObr). (2004, 2015, 2020). *Uradni list RS*, (103/04, 95/15, 139/20).

Zakon o preprečevanju pranja denarja in financiranja terorizma (ZPPDFT-2). (2022). *Uradni list RS*, (48/22, 145/22).

Zakon o splošnem upravnem postopku (ZUP). (2006, 2007, 2008, 20010, 2013, 2020, 2022). *Uradni list RS*, (24/06, 105/06, 126/07, 65/08, 8/10, 82/13, 175/20, 3/22).

Zakon o tajnih podatkih (ZTP). (2001, 2006, 2010, 2011, 2020, 2023). *Uradni list RS*, (87/01, 50/06, 9/10, 60/11, 8/20, 18/23).

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

Zakon o varovanju osebnih podatkov (ZVOP-2). (2022). *Uradni list RS*, (163/22).

Zakon o varstvu okolja (ZVO-2). (2022, 2023, 2024). *Uradni list RS*, (44/22, 78/23, 23/24).

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

O avtorjih:

Karmen Černigoj, Ministrstvo za vzgojo in izobraževanje, e-pošta: karmen.cernigoj@student.um.si

Dr. Miha Dvojmoč, Univerza v Mariboru, Fakulteta za varnostne vede, e-pošta: miha.dvojmoc@um.si