



# INFORMACIJSKA VARNOST: DOBA TEHNOLOŠKIH PREBOJEV IN PRAVNIH IZZIVOV

Urednik: Blaž Markelj

LEXPERA®

**GV**  
ZALOŽBA

Ljubljana 2023



# Predgovor

Knjiga *Informacijska varnost: Doba tehnoloških prebojev in pravnih izzivov* je tretja v zbirki *Informacijska varnost*. Obravnava številne informacijskovarnostne probleme, tudi v povezavi s pravnimi vidiki. Kot družba smo danes vsepovsod obkroženi z novodobno tehnologijo, ki nam v vsakdanjem življenju na vsakem koraku želi »pomagati«. Nova tehnologija pa poleg pozitivnih stvari prinaša tudi nevarnosti. Te se lahko kažejo kot poseg v posameznikovo zasebnost, nedovoljena odtujitev podatkov, analiziranje uporabnikovega obnašanja, povzročanje materialne škode itn. Zato je pomembno, da kot družba poznamo tehnologijo, ki jo uporabljamo, in začrtamo mejo, do katere je njena uporaba pravno dovoljena. V knjigi so obravnavane številne problematike, s katerimi se srečujemo že danes ali nas čakajo v prihodnosti. Poleg tega je poznavanje preteklosti in sedanjosti izredno pomembno za varno in preudarno uporabo tehnologije v prihodnosti. Knjiga nam ponuja vpogled v svet informacijske varnosti s predstavitvijo povezljivosti posameznika, družbe in tehnologije.

Prvo poglavje nas popelje v družbo 5.0 in predstavi, kako smotrno ravnati z informacijami v kibernetnem prostoru in kateri izzivi nas čakajo pri zagotavljanju informacijske varnosti. V ospredje postavlja temelje sobivanja med resničnim in virtualnim svetom, kamor pri uporabi kibernetnega sveta kot družba vstopamo. Digitalizacija družbe je namreč v polnem teku, na vsakem koraku se srečujemo z novodobno tehnologijo, ki na novo oblikuje gospodarsko panogo in hkrati tudi samo družbo. Oblikovanje uravnoteženih informacijskovarnostnih razmerij med tehnologijo in družbo ter posameznikom, ki pomeni samo središče uporabe tovrstne tehnologije v kibernetnem

prostoru, je velik izziv, s katerim se moramo spopasti že zdaj, v prihodnje pa bo ta izziv še večji.

Drugo in tretje poglavje obravnavata področje informacijske varnosti in testiranja odpornosti sistemov. Drugo se tako usmerja v informacijsko varnost portala eUprava in to povezuje tudi s pravnimi vidiki, medtem ko je v tretjem poglavju pozornost namenjena preverjanju informacijske varnosti s predstavitevjo etičnega hekanja tudi v okvirih kazenskega prava. Etično hekanje avtorji predstavijo kot večplastno preverjanje informacijske varnosti sistemov. Tako preverjanje pa je treba zelo dobro opredeliti tudi v zakonodaji. Poznavanje kazenskopравnih vidikov zagotavljanja kibernetске varnosti sistemov je zato še toliko pomembnejše.

Četrto poglavje je namenjeno hibridnim ogrožanjem, ki jih avtor definira kot uporabo sinhrono povezanih aktivnosti s cilji političnih, ekonomskih, finančnih in ozemeljskih interesov. Zadnje, peto poglavje pa nam podrobneje predstavi tehnologijo prepoznave obraza, ki jo uporablja policija. V njem avtor opredeli pravne vidike uporabe te tehnologije v povezavi s posegom v posameznikovo zasebnost in tehnološko opredelitvijo samih sistemov. Poudarjene so dileme uporabe tovrstne tehnologije, povezane s številnimi željnimi uporabniki na eni strani in stopnjo posega v zasebnost uporabnika, ki je glede zakonodaje še dovoljena, na drugi.

V knjigi so predstavljene pomembne tehnološke in pravne ugotovitve, ob tem pa so obravnavani številni novi pravni izzivi, povezani s hitrim razvojem današnje tehnologije. Zagotavljanje varnosti informacij in informacijske varnosti ter s tem posameznikove zasebnosti je kljub napredni pametni tehnologiji mogoče. Tudi z uporabo pravnih vidikov, ki začrtujejo »okvir«, v katerem se posameznik in družba gibljeta v kibernetsem prostoru.

izr. prof. dr. Blaž Markelj

*Fakulteta za varnostne vede Univerze v Mariboru*

# Kazalo

|          |   |    |
|----------|---|----|
| <b>1</b> | <b>Izzivi informacijske varnosti pri prehodu v družbo 5.0</b>       |    |
|          | <i>Igor Bernik</i> .....  | 13 |
| 1.1      | Uvod .....  | 13 |
| 1.2      | Izzivi družbe 5.0 .....   | 17 |
| 1.2.1    | Informacijska varnost .....   | 17 |
| 1.2.2    | Zbiranje in uporaba podatkov .....                                  | 19 |
| 1.2.2.1  | Internet stvari (IoT) .....   | 20 |
| 1.2.2.2  | Obsežni podatki ( <i>big data</i> ) .....                           | 21 |
| 1.2.2.3  | Uporaba umetne inteligence (UI) .....                               | 24 |
| 1.2.2.4  | Obvladovanje kibernetских groženj .....                             | 26 |
| 1.2.3    | Umestitev posameznika v središče razvoja .....                      | 28 |
| 1.2.3.1  | Informacijska varnost in podatkovna zasebnost .....                 | 29 |
| 1.2.3.2  | Usposabljanje in ozaveščanje .....                                  | 30 |
| 1.3      | Sklep .....   | 31 |
|          | Viri in literatura .....  | 33 |
| <b>2</b> | <b>E-vdori v eUpravo</b>  |    |
|          | <i>Gorazd Praprotnik, Blaž Markelj</i> .....                        | 35 |
| 2.1      | Uvod .....  | 35 |
| 2.2      | Zakonodaja na področju kibernetске varnosti .....                   | 37 |
| 2.2.1    | Analiza zakonodaje na področju kibernetске varnosti – eUprava ..... | 39 |
| 2.3      | Kibernetски napadi .....  | 46 |
| 2.3.1    | Rast kibernetских napadov .....                                     | 48 |
| 2.3.2    | E-vdori kot problematični kibernetски napadi ..                     | 49 |

|          |  |     |
|----------|--|-----|
| 2.4      | Portal eUprava .....   | 51  |
| 2.5      | Sistem SI-PASS.....  | 51  |
| 2.6      | Primernost prijave v portal eUprava prek SI-PASS .....   | 52  |
| 2.6.1    | Varnost uporabe sistema SI-PASS .....  | 53  |
| 2.6.2    | Varnostni vidik uporabe kvalificiranega digitalnega potrdila za identifikacijo in overjanje..... | 54  |
| 2.6.3    | Anonimna prijava v SI-PASS.....  | 56  |
| 2.6.4    | Anonimna prijava v SI-PASS prek posredniškega strežnika.....                                     | 57  |
| 2.6.5    | Anonimna prijava v SI-PASS prek omrežja TOR .....  | 60  |
| 2.6.6    | Problematika zavarovanja elektronskih sledi po e-vdoru .....                                     | 62  |
| 2.6.7    | Problematika shranjevanja uporabnikovih podatkov kot dokaznega materiala .....                   | 63  |
| 2.7      | Prihod kvantnih računalnikov .....   | 63  |
| 2.8      | Razprava .....   | 65  |
| 2.9      | Sklep .....  | 67  |
|          | Viri in literatura .....   | 67  |
| <b>3</b> | <b>Etično hekanje: varnostna in kazenskopravna vprašanja</b>                                     |     |
|          | <i>Sara Tomše, Sabina Zgaga Markelj, Blaž Markelj</i> .....                                      | 71  |
| 3.1      | Uvod .....   | 71  |
| 3.2      | Hekanje.....   | 75  |
| 3.2.1    | Etično hekanje .....   | 76  |
| 3.2.2    | Kazenskopravni vidiki etičnega hekanja .....   | 78  |
| 3.3      | Mnenjska raziskava o etičnem hekanju v Sloveniji.....  | 84  |
| 3.4      | Razprava.....  | 95  |
| 3.5      | Sklep .....  | 97  |
|          | Viri in literatura .....   | 100 |

|          |   |     |
|----------|---|-----|
| <b>4</b> | <b>Hibridna ogrožanja in ugrabitev zakonodaje</b>   |     |
|          | <i>Bojan Dobovšek</i> .....   | 105 |
| 4.1      | Prolog .....  | 105 |
| 4.2      | Ugrabitev zakonodaje .....  | 109 |
| 4.2.1    | Tarče, nosilci in sredstva »prevzema«<br>in »vpliva« .....  | 114 |
| 4.2.2    | Strategije za uveljavljanje vpliva .....  | 117 |
| 4.3      | Sklep .....   | 118 |
|          | Viri in literatura .....  | 121 |
| <b>5</b> | <b>Tehnologija prepoznave obrazov v rokah policije:<br/>zaupanje v tehnologijo je zaupanje v policijo</b> |     |
|          | <i>Jernej Lavrenčič</i> .....   | 125 |
| 5.1      | Namesto uvoda – drama v treh dejanjih .....   | 125 |
| 5.2      | Splošno o tehnologiji prepoznave obrazov .....  | 127 |
| 5.2.1    | FRT in biometrija .....   | 127 |
| 5.2.2    | Identifikacija in avtentifikacija .....   | 129 |
| 5.2.3    | Kaj je biometrični podatek .....  | 130 |
| 5.2.4    | (Ne)zanesljivost in stopnja ujemanja .....  | 132 |
| 5.3      | Normativna ureditev obdelave biometričnih podatkov ..   | 134 |
| 5.3.1    | Evropska unija .....  | 134 |
| 5.3.2    | Slovenska ureditev .....  | 136 |
| 5.4      | FRT v policijskem delu .....  | 138 |
| 5.4.1    | Identifikacija v retrospektivi (Clearview AI) .....   | 139 |
| 5.4.1.1  | Pravna dopustnost v EU .....  | 140 |
| 5.4.1.2  | Odziv evropskih organov za varstvo<br>osebnih podatkov .....  | 142 |
| 5.4.2    | Prepoznavna obrazov v realnem času<br>(AFR Locate) .....  | 143 |
| 5.5      | Posegi v človekove pravice s FRT .....  | 145 |
| 5.5.1    | Splošno .....   | 145 |

|         |   |            |
|---------|---|------------|
| 5.5.2   | Pravica do zasebnega življenja (zasebnosti) . . .   | 146        |
| 5.5.3   | Pravica do varstva osebnih podatkov . . . . .   | 149        |
| 5.5.3.1 | Splošno . . . . .   | 149        |
| 5.5.3.2 | Ustavnosodna presoja . . . . .  | 153        |
| 5.5.4   | Pravica do nediskriminatornega<br>obravnavanja . . . . .                                  | 156        |
| 5.5.5   | Pravica do zbiranja in svoboda izražanja . . . . .  | 157        |
| 5.5.6   | Pravica do (učinkovitega) pravnega sredstva . .   | 159        |
| 5.6     | Namesto sklepa – kategorično prepovedana uporaba<br>FRT ali le strogo zamejena? . . . . . | 159        |
|         | Viri in literatura . . . . .  | 162        |
|         | <b>Povzetki . . . . .</b>   | <b>169</b> |
|         | <b>O avtorjih . . . . .</b>   | <b>175</b> |
|         | <b>Recenziji . . . . .</b>  | <b>179</b> |

## Kazalo slik

|            |  |    |
|------------|--|----|
| Slika 2.1: | Število obravnavanih incidentov po letih . . . . .   | 49 |
| Slika 2.2: | Lista posredniških strežnikov . . . . .  | 57 |
| Slika 2.3: | Prijava v spletni portal SI-PASS prek posredniškega<br>strežnika . . . . .                         | 58 |
| Slika 2.4: | Poštni predal začasne pošte z obvestilom<br>o registraciji uporabnikovega računa SI-PASS . . . . . | 59 |
| Slika 2.5: | Obvestilo o uspešnosti prijave v register centralnega<br>prebivalstva . . . . .                    | 60 |
| Slika 2.6: | Prijava v portal SI-PASS prek brskalnika TOR. . . . .  | 61 |
| Slika 2.7: | Povezava med varnostjo sistema, udobjem<br>in zasebnostjo uporabnika . . . . .                     | 66 |
| Slika 3.1: | Samoocena računalniškega znanja . . . . .  | 86 |

|   |     |
|---|-----|
| Slika 3.2: Cronbachov koeficient alfa zanesljivosti . . . . .                                 | 87  |
| Slika 3.3: Opisna statistika za sklop Koristnost etičnega hekanja . . . . .                   | 88  |
| Slika 3.4: Rezultati parnega t-testa . . . . .  | 89  |
| Slika 3.5: Povzetek večkratne regresije . . . . .   | 90  |
| Slika 3.6: Opisna statistika za sklop Ustreznost informacijske varnosti v podjetjih . . . . . | 91  |
| Slika 3.7: Povzetek regresijske analize . . . . .   | 91  |
| Slika 3.8: Opisna statistika za sklop Lastnosti hekerjev . . . . .                            | 92  |
| Slika 3.9: Rezultat t-testa (lastnosti hekerjev) . . . . .                                    | 93  |
| Slika 3.10: Opisna statistika za sklop Zakonska ustreznost informacijske varnosti . . . . .   | 93  |
| Slika 3.11: Rezultat t-testa (zakonska ustreznost informacijske varnosti) . . . . .           | 94  |
| Slika 3.12: Koeficienti korelacije . . . . .  | 95  |
| Slika 4.1: Mehanizmi korupcije, »prevzema« in »vpliva« . . . . .                              | 116 |
| Slika 4.2: Vplivi nedržavnih akterjev na državne akterje . . . . .                            | 118 |



# Recenziji

Znanstvena monografija *Informacijska varnost: Doba tehnoloških prebojev in pravnih izzivov* je sestavljena iz petih poglavij, ki so jih napisali različni avtorji in so vsako zase znanstvena zaključena celota o posamezni problematiki informacijske varnosti. Poglavlja so:

1. Izzivi informacijske varnosti pri prehodu v družbo 5.0
2. E-vdori v eUpravo
3. Etično hekanje: varnostna in kazenskoppravna vprašanja
4. Hibridna ogrožanja in ugrabitev zakonodaje
5. Tehnologija prepoznave obrazov v rokah policije: zaupanje v tehnologijo je zaupanje v policijo

Poglavlja znanstvene monografije so med seboj smiselno povezana v celoto, hkrati pa je vsako zase strokovno in raziskovalno zaključena celota. Naslov monografije nakazuje, da se bo vsebinsko dotaknila preteklosti, sedanjosti in predvsem prihodnosti tehnološkega razvoja digitalnih tehnologij v razmerju z razvojem prava. Pravo namreč postavlja norme, v okviru katerih naj bi posameznik in družba pri uporabi kibernetnega prostora delovala. Osrednja pozornost v monografiji je namenjena zagotavljanju informacijske varnosti, posameznikovi zasebnosti ter oblikovanju in uveljavljanju ustrezne zakonodaje. Avtorji postavijo pomembna strokovna in raziskovalna izhodišča glede povezave med informacijsko varnostjo in pravom, ki so družbeno koristna. Zato je tovrstna literatura pomembno gradivo, ki je strokovni, študentski in znanstveni javnosti lahko v pomoč pri identifikaciji in reševanju problematike, s katero se posameznik in družba srečujeta v povezavi z uporabo sodobne tehnologije in varovanjem posameznikove in družbene zasebnosti.

Menim, da je znanstvena monografija po vsebini, strukturi in zastavljeni zasnovi dela ustrezna, in predlagam njeno izdajo.

zasl. prof. dr. Vladislav Rajkovič  
Fakulteta za organizacijske vede Univerze v Mariboru

Ljubljana, 7. maja 2023

\* \* \*

Delo *Informacijska varnost: Doba tehnoloških prebojev in pravnih izzivov* je znanstvena monografija, ki jo sestavlja pet poglavij. Vsako poglavje je sklenjena celota, poglavja pa se vsebinsko lepo povezujejo med seboj. Rdeča nit knjige sta skrb za informacijsko varnost ob današnji hitro razvijajoči se tehnologiji in pravna podlaga, ki določa pravila delovanja posameznika in družbe v kibernetnem prostoru. Prvo poglavje monografije obravnava družbo 5.0 ter današnjo digitalizacijo družbe in zagotavljanje informacijske varnosti pri uporabi kibernetnega prostora. Avtor v središče poglavja postavi vpliv digitalizacije na družbo s posameznikom na eni strani ter oblikovanjem razmerij med družbo in tehnologijo na drugi. V drugem in tretjem poglavju avtorji obravnavajo pomen preverjanja varnosti posameznih informacijskih sistemov, tudi z metodo etičnega hekinga, vendar, kot poudarjajo, vedno v legalnih, pravno »varnih« okvirih. Četrto poglavje je namenjeno hibridnim grožnjam, ki imajo vedno neki namen. V zadnjem, petem poglavju so predstavljene pravne dileme glede uporabe tehnologije prepoznavne obraza; postavlja se vprašanje posega v posameznikovo zasebnost pri uporabi tovrstne tehnologije.

Znanstvena monografija že v prvem poglavju postavi zanimiva vprašanja, o katerih bi morali razmišljati vsi uporabniki današnje digitalne tehnologije, tj. o tem, kje so meje tovrstne tehnologije v povezavi s posameznikovo zasebnostjo in širše zagotavljanjem informacijske

varnosti. V nadaljevanju je ta tematika poglobljeno obravnavana ob predstavitvi tveganj pri uporabi tovrstne tehnologije, knjiga pa se zaključí z obravnavo pravnih vprašanj o uporabi biometrične tehnologije prepoznave obraza.

Znanstvena monografija *Informacijska varnost: Doba tehnoloških prebojev in pravnih izzivov* je izredno pomembno gradivo tako za posameznika kot za družbo in bi jo priporočil v branje vsakemu uporabniku današnje digitalne tehnologije oziroma kibernetškega prostora. Glede na vsebino in strukturo izpolnjuje kriterije znanstvene monografije, zato predlagam njeno izdajo.

izr. prof. dr. Janez Mekinc  
Fakulteta za turistične študije –  
Turistica Univerze na Primorskem

Ljubljana, 4. maja 2023

## Mnenja o knjigi

Tehnološki preboji, ki smo jim priča v zadnjih dveh desetletjih, nas navdajajo s pisano paleto občutkov. Prav vsem pa je skupno, da njihove uporabnosti v vsakdanjem življenju nikakor ne moremo zanikati. Vseprisotnost tehnologije in skoraj neomejene možnosti, ki jih ponuja tako posameznikom kot podjetjem, vedno znova postavljajo nova vprašanja v polju informacijske varnosti. Namen informacijske varnosti je preprečiti, da bi se zgodilo nekaj neželenega, torej delovati preventivno in v družbeno korist. Kljub temu je pomembno upoštevati vse vidike ter tehnologijo v povezavi z informacijsko varnostjo osmisлити tudi v pravnih okvirih – samo tako bo družba s tehnologijo živela v odnosu, utemeljenem na zaupanju. Knjiga, ki jo imate pred seboj, ponuja prav to. Opremila vas bo z razumevanjem te kompleksne dihotomije in opolnomočila s konkretnimi znanji za lažje sobivanje v resničnem in virtualnem svetu.

**Matej Matija Grobelšek**, direktor za poslovni trg, A1 Slovenija, d. d.

V današnjem času hitrega razvoja in digitalizacije družbe, ko tehnologija vse večkrat prehiteva pripravljenost družbe in zakonodaje na morebitne posledice, ki jih ta razvoj prinaša, je tovrstna monografija zelo dobrodošla. V knjigi je pet poglavij, ki vsako zase celovito obravnavajo aktualne teme in ponudijo vpogled v izzive uporabe ali uvedbe tehnologije, tveganja, ki jih tehnologija prinaša, in zakonske okvire v evropskem pravnem prostoru. Spoznali boste izzive informacijske varnosti pri prehodu družbe na novo digitalno raven, stanje aktualne eUprave ter izzive, s katerimi se srečujejo pri različnih storitvah za prebivalce, etično hekanje in njegove meje, hibridna ogrožanja pri vplivih na zakonodajo ter tehnologijo za prepoznavo obrazov, ki je zanimiva tema tako pri nas kot po svetu. Pri informa-

cijski varnosti vedno skušamo najti ravnovesje med ustrezno zaščito na eni strani in vzdržnostjo »normalnega« poslovanja na drugi, za ravnovesje pri uporabi in vpeljavi novih tehnologij in rešitev pa je zelo pomembno poznati tudi pravne dileme in vidike. Pri tem vam bo knjiga zagotovo pomagala.

**Bojan Brodar**, direktor informacijske varnosti,  
*Telemach Slovenija, d. o. o.*

Strokovnjaki za informacijsko varnost pri svojem delu vsak dan srečujemo najrazličnejše izzive. Največkrat se ukvarjamo s tehnološkimi in administrativnimi ukrepi, s katerimi znižujemo oceno tveganja. Pri tem se občasno zgodi, da prezremo pravni vidik. Ukrepi lahko postanejo nesorazmerni in pretirano posežejo v posameznikovo zasebnost. Zato bo knjiga obvezno branje za vsakega vodjo, ki se ukvarja z informacijsko varnostjo, priporočam pa jo tudi varnostnim inženirjem.

**Žiga Humar**, CISSP, vodja ekipe za informacijskovarnostne rešitve,  
*Our Space Appliances, d. o. o.*

Vedno v zgodovini so se pojavljale prebojne tehnologije in rešitve. Danes je to generativna umetna inteligenca, ki intenzivno vstopa v naše vsakdanje življenje. Jutri bo to kvantno računalništvo in še vrsta drugih pomembnih tehnoloških dosežkov. Toda ali smo kot posamezniki in družba dovolj zreli, da jih bomo znali uporabljati pravilno in etično? Tudi če smo, pa se vedno najdejo posamezniki in skupine, ki to tehnologijo želijo zlorabljeni za svoje neetično ali celo nezakonito početje. Za opredelitev, kdaj je neko početje nezakonito, seveda potrebujemo zakonodajo, ki bo ta nova področja obravnavala tako, da bo dopuščala razvoj in koristno uporabo ter onemogočala in sankcionirala zlorabo. Knjiga v petih poglavjih obravnava te nove tehnologije in z njimi povezane aktivnosti ter postavlja zelo pomembna vprašanja, kako jih obvladovati s pravnega vidika. Monografija si prav zaradi povezovanja med področjema tehnologije in

prava, kar je nazorno predstavljeno na konkretnih primerih, zasluži posebno pozornost.

**Metod Platiše**, vodja centra kibernetске varnosti v prodaji, Telekom Slovenije, d. d.

Zdi se, kot da smo tik pred novo industrijsko revolucijo. Spodbudila jo bosta digitalna preobrazba različnih družbenih (pod)sistemov in razvoj (uporabne) umetne inteligence. Kot vse industrijske revolucije doslej bo močno vplivala na posameznike, na njihovo življenje in delo ter na odnose med ljudmi v vse bolj povezanem in avtomatiziranem okolju. Ob navdušenju nad tehnologijo in prizadevanji za še hitrejši tehnološki razvoj pa nikakor ne smemo pozabiti na človeka in na družbene dosežke naših prednikov. V času sprememb moramo nujno razviti tudi zavedanje o informacijskovarnostnih tveganjih in drugih z njimi povezanih izzivih, kot so zasebnost, nadzor, svoboda, varnost, pravni vidiki ipd., da jih bomo lahko ustrezno obravnavali. Te in podobne teme predstavi ta knjiga, za osvežitev lekcij iz zgodovine pa bo treba poseči po drugih virih.

**dr. Boris Horvat**, direktor, Abelium, d. o. o.

Znanstvena monografija Informacijska varnost: Doba tehnoloških prebojev in pravnih izzivov je nastala v zelo primernem času – v zadnjih letih smo priča izjemnim napredkom tehnologije, zlasti na področju umetne inteligence, ki bodo korenito spremenili svet, v katerem živimo. Ali in pod kakšnimi pogoji bomo dovolili, da o našem zdravljenju, o primernosti za pridobitev kredita ali socialnih transferjev odločajo črne škatle, katerih delovanje težko razložijo že ustvarjalci, kaj šele posamezniki, katerih pomembni deli življenja bodo podvrženi algoritmom umetne inteligence? Kako ustrezno regulirati druge tehnološke izzive, kakršen je na primer prepoznavo obrazov na javnih površinah, in katera tveganja za varnost naših podatkov prinašajo pametna mesta in internet stvari? S podrobno obravnavo omenjenih tem monografija prispeva k strokovni in splo-

šni razpravi o tem, kako izrabiti prednosti novih tehnologij in obenem omejit morebitne negativne posledice, ter o tem, v kakšnem svetu si pravzaprav želimo živeti.

**Mojca Prelesnik**, informacijska pooblaščenka RS

Knjiga ni pomemben pripomoček samo za tiste, ki se ukvarjajo z informacijsko varnostjo, ampak tudi za širšo družbo. Opozarja namreč na pomembnost ravnanja z informacijami v digitalnem svetu in nas seznanja z izzivi pri zagotavljanju informacijske varnosti. Tega se mora zavedati čim širša družba, ne le nekaj strokovnjakov s tega področja, saj samo s širšim poznavanjem dilem v kibernetičnem svetu lahko kot družba poskrbimo za ustrezno informacijsko varnost. Knjigo zato priporočam v branje vsem, ki želijo izboljšati svoje ravnanje z digitalnimi informacijami, se seznaniti s prihajajočimi izzivi na področju informacijske varnosti ter si ogledati varnost tudi na konkretnih primerih.

**mag. Jure Valjavec**, predsednik posloводства, T-2, d. o. o.

Kot direktor podjetja, ki že več kot tri desetletja vzpostavlja zanesljiva in predvsem varna poslovna in procesna komunikacijsko-informacijska omrežja, še posebej pozdravljam prepotrebno izdajo takšnega strokovnega vpogleda v informacijsko varnost. Pod skrbnim uredništvom dr. Blaža Marklja so nam predstavljeni izzivi obvladovanja kibernetičnih groženj, zbiranja in uporabe podatkov, vpeljave umetne inteligence, umestitve posameznika v središče tehnološkega razvoja in varnostne zakonodaje na področju informacijske varnosti. Knjigo priporočam vsem, ki želijo bolje razumeti izzive informacijske varnosti v družbi 5.0, okrepiti kibernetično zaščito in učinkoviteje obvladovati sodobne kibernetične grožnje s pravnega vidika.

**Jure Remškar**, izvršni direktor, Smart Com, d. o. o.

Tudi v tretji knjigi iz zbirke so obravnavane teme celostno predstavljene, s poudarkom na potrebi po usklajenosti med pravnimi in tehnološkimi vidiki. Avtorji pri obravnavi posameznih tematik v svojih poglavjih v ospredje postavljajo posameznika. Temu naj informacijska tehnologija pomaga dosegati poslovne in osebne cilje. Vendar, kot je poudarjeno, uporabnik v kibernetnem prostoru nikoli ni sam. V boju proti kibernetnemu kriminalu po besedah avtorjev ključen ostaja interdisciplinarni pristop osrednjih deležnikov, od specialistov s področja informacijske varnosti do pravne doktrine. Osebo in tudi v vlogi vodje varnostnega operativnega centra, ki deluje doma in na tujem, takšno sodelovanje pozdravljam. Predvsem me veseli, da bodo po knjigi s tako aktualno temo lahko posegli vsi mladi bralci, ki v iskanju svoje nadaljnje karijerne poti še iščejo svoj prispevek družbi. Tisto nekaj, česar v šolskih klopeh ali ob prebiranju pogosto recikliranih novičk z malih zaslonov ne izvemo, je v knjigi mojstrsko podano. Priporočam.

**mag. Matevž Mesojednik**, vodja varnostnega operativnega centra,  
NIL, d. o. o.

Tehnologija in z njo povezana digitalna preobrazba spreminjata naša življenja na boljše. Živimo v tako imenovani digitalni dobi, tehnologija je postala neločljiv del življenja, tako na osebnem kot na poslovnem področju. Ključna pa je usposobljenost posameznika, družbe in gospodarstva za uporabo tehnologije, pri čemer ne smemo pozabiti na elementa varnosti in zasebnosti. Tehnologija se razvija hitreje, kot ji sledi pravna zakonodaja, ki digitalno okolje ureja. Samo digitalno okolje pa mora posamezniku zagotavljati pravico do zasebnosti in varovati njegove osebne podatke. V knjigi so nova področja, ki jih omogoča tehnologija, razumljivo predstavljena, v ospredje pa so postavljeni uporabnik tehnologije, etični vidik, varnost in zasebnost.

**Vida Dolenc Pogačnik**, direktorica operative in mednarodnega sodelovanja, AmCham Slovenija