

# НОРМАТИВНО УРЕЂЕЊЕ УПРАВЉАЊА КОНТИНУИТЕТОМ ПОСЛОВАЊА У РЕПУБЛИЦИ СРБИЈИ

маст. Јана Марковић, докторант\*  
Универзитет у Београду, Факултет безбедности

---

\* 1996janamarkovic@gmail.com



## НОРМАТИВНО УРЕЂЕЊЕ УПРАВЉАЊА КОНТИНУИТЕТОМ ПОСЛОВАЊА У РЕПУБЛИЦИ СРБИЈИ

**Сажетак:** *Проблем који се обрађује у овом раду тиче се континуитета пословања, односно управљања континуитетом пословања. Управљање континуитетом пословања се може схватити као једна од основних функција сваке организације чије је успостављање и остваривање нужно за обезбеђивање наставка пословања и уједно функционисања организације у случају било каквог ометања изазваног потенцијално штетним догађајем. Са друге стране, није погрешно ову функцију разумети као интегрални део корпоративне безбедности. У овом раду пошло се од истраживачког питања да ли у Републици Србији постоји адекватан нормативни оквир управљања континуитетом пословања. Аутор је у раду истраживао да ли је на задовољавајући начин нормативно уређен процес управљања континуитетом пословања, конкретно правних прописа Републике Србије, стандарда у овој области, али и прописа на нивоу Европске уније, како би се утврдиле релевантне одредбе које недостају у законодавству Републике Србије. Очекивани резултат јесте да се на основу свеобухватне анализе садржаја докумената који регулишу управљање континуитетом пословања за Републику Србију, а потом и на нивоу који превазилази границе државе – за међународну заједницу у области континуитета пословања креирану од стране државних и недржавних ентитета који за циљ имају свеобухватније разумевање и примењивање концепта континуитета пословања. Све до сада изнето аутор користи како би у закључним разматрањима указао на нормативно уређење предметне области у Републици Србији, али и шире, на значај целокупне области континуитета пословања, као и на значај веће укључености државе у регулисање питања ове врсте.*

**Кључне речи:** *организациона функција, управљање континуитетом пословања, правни прописи, стандарди.*

### Увод

Континуитет пословања је релативно нов појам у стручној и научној литератури и могу се издвојити различити приступи и дефиниције. Ипак, овде ћемо представити само оне које нам дају јасан и

прецизан садржај овог изузетно важног процеса у пословању организација, али и саме државе. Дакле, управљање континуитетом пословања може се дефинисати као процес који идентификује „изложеност организације унутрашњим и спољним претњама” (Herbane et al., 2004: 435), могуће последице (Cornish, 2010), одређује „процесе и људе који су пресудни за опстанак организације” (Randeree et al., 2012: 473), неопходне ресурсе, а све у циљу спречавања губитака и припреме за ублажавање и управљање поремећајима (International Organization for Standardization, 2020).

Најопштије речено, континуитет пословања јесте функција која осигурава наставак пословања организације у случају непредвиђених догађаја попут криза, обезбеђујући њено непрекидно функционисање. Иако је функција управљања континуитетом пословања развијена превасходно за организације, односно правна лица, и то пре свега за оне које доходују/приходују, односно остварују профит, континуитет пословања се може разматрати и у контексту непрекидног функционисања државе и државног апарата кроз деловање, пре свега, државне управе, као власти, службе и регулатора друштвених процеса.

Анализа нормативног оквира на коју је стављен фокус у овом раду обухватиће три дела. Први део обухвата анализу правних прописа којима је приступљено са Правно-информационог система Републике Србије, и то доступни стратегијско-доктринарни документи, закони и прописи донети на основу закона у областима које ће бити наведене у раду. Други део се односи на анализу стандарда у области континуитета пословања и трећи обухвата анализу прописа на нивоу Европске уније.

## Правни прописи Републике Србије

С обзиром на то да се континуитет пословања суштински односи на организације, или конкретније правна лица<sup>1</sup>, анализом најпре треба обухватити прописе којима се регулише рад тих ентитета. Ниједно правно лице не може постојати и функционисати (пословати) уколико не испуњава услове које прописује позитивно законодавство и

1 Организација је шири појам од појма правног лица, узимајући у обзир да организација може добити статус правног лица у оквиру правног поретка државе. Конкретно, организација постаје правно лице када добије правни субјективитет, односно када јој се признају правна, пословна и деликтна способност, што се у Републици Србији постиже уписом у регистар Агенције за привредне регистре (Милошевић, 2012: 148).

уколико се не придржава основних прописа којима се уређује њихов рад, као и прописа специфичних за делатност коју врше. Основни пропис којим се регулише рад свих правних лица у нашој земљи јесте Закон о привредним друштвима.<sup>2</sup> Поред њега, правна лица имају обавезу поштовања, за њихову делатност, специфичних прописа. Анализом у овом раду, а која је задржана на Закону о привредним друштвима и актима који су донети на основу истог, утврђено је да не постоји одредба која би директно или посредно упућивала на било који сегмент управљања континуитетом пословања.

Уколико се, пак, за анализу узму прописи у два области – информационе технологије и Народна банка и банке и друге финансијске организације<sup>3</sup>, у којима се концепт управљања континуитетом пословања првобитно развијао (Borodzicz, 2005; Herbane, 2010), закључак је другачији.

У области информационих система од значаја за предмет рада јесу Закон о информационој безбедности и Уредба о ближе уређењу мера заштите информационо-комуникационих система од посебног значаја. На основу ових докумената посебно се издвајају следеће одредбе: једне од мера заштите ИКТ система јесу мере које обезбеђују континуитет обављања посла у ванредним околностима (члан 7 став 3 тачка 28 Закона о информационој безбедности, 2016); дужности оператора ИКТ система у погледу инцидената везаних за прекид континуитета или тешкоћа у вршењу послова и пружању услуга (члан 11а Закона о информационој безбедности, 2016); дужности оператора ИКТ система у погледу мера које обезбеђују континуитет обављања посла у ванредним околностима (члан 29 Уредбе о ближе уређењу мера заштите информационо-комуникационих система од посебног значаја, 2016); дужности Националног ЦЕРТ-а<sup>4</sup> у циљу обезбеђивања континуитета рада (члан 15 став 6 Закона о информационој безбедности, 2016).

Поједини прописи донети у оквиру финансијског сектора такође садрже одредбе које се тичу управљања континуитетом пословања. Издваја се Закон о банкама, а нарочито његови сегменти који се односе на план реструктурирања банке (члан 128в) и процену могућности реструктурирања (члан 128д), где се ставља акценат на обезбеђивање

2 Позитивно законодавство Републике Србије користи термин *привредно друштво* које означава „правно лице које обавља делатност у циљу стицања добити” (члан 2 Закона о привредним друштвима, 2011).

3 Називи области су преузети са сајта Правно-информационог система Републике Србије који је коришћен за анализу као база домаћих правних прописа.

4 Национални центар за превенцију безбедносних ризика у ИКТ системима Републике Србије.

континуитета у обављању критичних функција банке, што је и један од циљева реструктурирања (члан 128а став 1 тачка 1 Закона о банкама, 2005). Даље, Одлуком о плановима опоравка банке и банкарске групе предвиђа се да саставни део плана опоравка (банке и банкарске групе) мора садржи активности и мере којима се обезбеђује континуитет у обављању активности (члан 9), као и поступке којима се обезбеђује континуитет пословања у случају примене неке од опција за опоравак (члан 11 Одлуке о плановима опоравка банке и банкарске групе, 2015). За наш предмет истраживања од посебног значаја је и Одлука о управљању ризицима банке, која доводи у везу континуитет пословања са концептом “going concern” (члан 27) и прописује обавезу банке да обезбеди континуитет критичних функција када намерава да трећем лицу повери активности чије је извршење значајно за обезбеђивање континуитета тих функција (члан 75 Одлуке о управљању ризицима банке, 2011). Вероватно највећи корак начињен у финансијском сектору, а који има везе са концептом управљања континуитетом пословања јесте усвајање Одлуке о минималним стандардима управљања информационим системом финансијске институције. Овом одлуком уређују се, између осталог, и минимални стандарди за управљање континуитетом пословања и опоравак активности у случају катастрофа у финансијској институцији (члан 1 став 2 Одлуке о минималним стандардима управљања информационим системом финансијске институције, 2013), што је посебно разрађено у глави 6 која обухвата и план континуитета пословања.

Из приложеног се може уочити да је, у одређеном обиму, управљање континуитетом пословања обухваћено прописима у областима информационих система и финансијског сектора. Управљање континуитетом пословања, укључујући план континуитета пословања, јесте концепт који је имплементиран у функционисање ИКТ система и финансијских институција. Међутим, наведено се не може рећи и за области које су „ближе” држави – за области одбране, војске и унутрашњих послова.

У стратегијско-доктринарним документима Републике Србије на свега неколико места се помиње континуитет, односно континуирано деловање. Примера ради, у Стратегији националне безбедности наглашава се неопходност за *континуираним* праћењем и анализом међународног окружења у контексту дефинисања изазова, ризика и претњи безбедности, као и *континуирана* опредељеност државе бављењем појединим питањима – национално јединство и развој

културног, верског и историјског идентитета и активности на сузбијању нелегалне трговине и акумулирања вишкова малог и лаког наоружања (Стратегија националне безбедности Републике Србије, 2019). Поред тога, у Стратегији одбране се на сличан начин помиње континуитет, овде у контексту неопходности *континуираног* развоја технолошке и информационе заштите елемената система одбране (Стратегија одбране Републике Србије, 2019). Слично је и са Стратегијом развоја Министарства унутрашњих послова за период 2018–2023. године, где се наглашава *континуираност* различитих активности које се предузимају ради остваривања циљева (Стратегија развоја Министарства унутрашњих послова за период 2018–2023. године, 2018). Међутим, наведени примери не одговарају схватању континуитета (пословања) који је предмет овог рада. Делимично, може се узети у обзир једно од начела система националне безбедности и система одбране – *непрекидност*, која обезбеђује остваривање функција ова два система „у континуитету, у миру, ванредном стању и рату, независно од околности које могу настати” (Стратегија националне безбедности Републике Србије, 2019; Стратегија одбране Републике Србије, 2019), и то само уколико следимо најопштији приступ континуитета (пословања). Поред наведеног, у Доктрини Војске Србије, иако се изричито не помиње континуирано деловање, указује се на непрекидно планирање, организовање и извођење обезбеђења Војске Србије у циљу реализације мисија и задатака (Доктрина Војске Србије, 2010), што омогућава њено деловање како у редовним тако и у ванредним приликама.

У законима и прописима донетим на основу закона у областима<sup>5</sup> одбрана и безбедност, војска Србије, полиција, јавни ред и мир и јавно окупљање, ванредне ситуације (цивилна заштита, елементарне и друге непогоде), заштита од пожара, детективска делатност и приватно обезбеђење, управљање континуитетом пословања није препознато као једна од значајних и неопходних функција којом се обезбеђује наставак пословања, или уопште функционисања, у случају каквих потенцијалних догађаја са негативним последицама. Делимичан изузетак јесте Закон о критичној инфраструктури, који обухвата управљање континуитетом пословања, али без изричите употребе овог термина. Наиме, закон представља заштиту критичне инфраструктуре као „скуп активности и мера које имају за циљ осигурање

5 Називи области су преузети са сајта Правно-информационог система Републике Србије који је коришћен за анализу као база домаћих правних прописа.

функционисања критичне инфраструктуре у случају ометања или уништења, односно заштиту у случају претњи и спречавање настанка последице ометања или уништења” (члан 2 став 1 тачка 4 Закона о критичној инфраструктури, 2018). Узимајући у обзир претходно изнетог, заштита критичне инфраструктуре, схваћена у контексту овог закона, садржи елементе карактеристичне за управљање континуитетом пословања. Начела деловања потврђују наведено обавезујући све надлежне субјекте да учествују у заштити критичне инфраструктуре пре, за време и после ометања или прекида у њеном функционисању, а на основу анализе ризика, да обезбеђују континуирани рад критичне инфраструктуре узимајући у обзир различите врсте ризика и да континуирано планирају заштиту критичне инфраструктуре, а опет на основу анализе ризика и процене адекватности мера заштите (члан 3 Закона о критичној инфраструктури, 2018). Из наведеног се може уочити потенцирање анализе ризика, што је од посебног значаја. Наиме, неизоставни део управљања континуитетом пословања јесте управо анализа ризика (Gibb & Buchanan, 2006), или прецизније анализа утицаја на пословање. Реч је о „анализи ресурса, система и операција организације” (Elliott, 2014: 824), односно анализи целокупног пословања која идентификује критичне ресурсе – оне тренутне и оне минималне за даље функционисање (Smith & Brooks, 2013) и функције, као и временски оквир у којима се они морају поново успоставити. Без обзира да ли се анализа посматрала као посебна фаза управљања континуитетом пословања (Elliott, 2014), или као саставни део планирања континуитета пословања (Karakasidis, 1997; Pitt & Goyal, 2004), омогућава реализовање даљих корака, од којих се нарочито истиче генерисање планова континуитета пословања.

План континуитета пословања треба да обухвати улоге и одговорности оних који ће реализовати план, мере и процедуре поступања, захтеве за ресурсе, захтеве за извештавање, координацију, комуникацију и остале неопходне информације за реализацију плана (International Organization for Standardization, 2019).

У анализираним законима и прописима може се уочити обавеза израде планова којима се уређује поступање у непредвиђеним ситуацијама, а у циљу избегавања ометања или прекида функционисања. Такав је, на пример, План одбране који садржи организацију снага, средстава, мера и поступака за рад државних органа и употребу Војске Србије и других снага одбране у ратном и ванредном стању (члан 81 став 2 Закона о одбрани, 2007).

Слично је и са Плановима заштите од пожара, који у неким својим деловима садрже елементе који подсећају на елементе планова континуитета пословања, попут утврђивања потребних ресурса, односно врсте и количине потребне опреме која ће се користити када пожар наступи (Правилник о начину израде и садржају Плана заштите од пожара аутономне покрајине, јединице локалне самоуправе и субјеката разврстаних у прву и другу категорију, 2010). Закон о смањењу ризика од катастрофа и управљању ванредним ситуацијама обавезује на израду раличитих планова попут Плана смањења ризика од катастрофа и Плана заштите и спасавања (Закон о смањењу ризика од катастрофа и управљању ванредним ситуацијама, 2018). Треба имати у виду да набројани планови, иако у неким својим сегментима могу садржати елементе који, како је већ назначено, подсећају на елементе планова континуитета пословања, ипак не представљају планове континуитета пословања у правом смислу. Чак и уколико би постојала потреба да се разврстају у неку од категорија активности субјеката, то би пре могла бити категорија планирања у непредвиђеним ситуацијама (contingency planning)<sup>6</sup>, што је шире од управљања континуитетом пословања.

Уколико анализирамо програме и планове превенције криминала, закључујемо да они такође садрже елементе које уочавамо у плановима континуитета пословања, попут анализе, активности које ће се предузети, носиоца тих активности, информације о координацији и комуникацији (члан 7 Правилника о начину обављања појединачних полицијских послова, 2018). Међутим, овакви планови не одговарају суштини управљања континуитетом пословања, јер се израђују за појаву која постоји и траје, а не за појаву, односно потенцијално штетни догађај за чије се превазилажење управљање континуитетом пословања и успоставља.

Поред наведеног, постоји обавеза правних лица од значаја за одбрану земље да планирају мере којима обезбеђују вршење производње и услуга, снабдевање сировинама, репроматеријалом, енергијом и другим потребама, потребан број радника за вршење производње и услуга и заштиту радника и материјалних и других добара и друге мере (члан 8 Одлуке о одређивању правних лица од значаја за одбрану Републике Србије, 2008; члан 8 Уредбе о начину и поступку извршавања

6 Комплетни програм планирања у непредвиђеним ситуацијама има три главна елемента: хитни одговор, кризни менаџмент и континуитет пословања – опоравак пословања и наставак пословања (Kovacich & Halibozek, 2003).

обавезе планирања припрема за одбрану, 2009), дакле да планирају своје ресурсе – снаге и средства, мере и поступке за рад, односно „утврђују шта је од виталног значаја за опстанак организације након велике катастрофе која утиче на нормално пословање” (Speight, 2011: 535), што је Спајт (Speight) препознао као планирање континуитета пословања.

Иако се анализирани нормативни оквир изричито не бави управљањем континуитетом пословања, државни органи у склопу својих надлежности имају право и обавезу предузимања активности којима ће се обезбедити опоравак од потенцијално штетних догађаја, попут елементарних и других непогода. Надлежни органи својим активностима обезбеђују наставак функционисања друштвеног живота и друштвене заједнице ограничавајући и уклањајући последице таквог штетног догађаја. Без обзира на то што би се овде могла уочити и функција кризног менаџмента обухватајући опоравак од кризе и функција континуитета пословања, имајући наведено на уму, могло би се рећи да држава преко својих органа обезбеђује континуирано функционисање заједнице и да као ентитет виши од правног лица спроводи функцију управљања континуитетом пословања, али на начин и у облику (форми) који је својствен њеним особеностима и њеној улози.

### **Стандарди у области управљања континуитетом пословања**

Други део анализе фокус ставља на међународне стандарде у области управљања континуитетом пословања, који прописују норме чије имплементирање и континуирана примена имају вишеструке користи за организацију. Основни стандард за управљање континуитетом пословања јесте међународни стандард<sup>7</sup> – *ISO 22301 Security and resilience – Business continuity management systems – Requirements* (у даљем тексту: ISO 22301), усвојен 2012. и ревидиран 2019. године, а настао од британског стандарда BS 25999. Овим стандардом се утврђују захтеви за примењивање, одржавање и побољшање система менаџмента ради заштите од поремећаја, смањења вероватноће њиховог појављивања, припреме и одговора на њих, као и опоравка од њих

<sup>7</sup> Назив овог и сваког наредног стандарда, као и документа остављен је на изворном енглеском језику, како не би дошло до евентуалне термилошке неусаглашености услед превођења.

када се појаве. Значај стандарда се огледа у томе што представља први међународни стандард у овој области, који је применљив на све организације или њихове делове, без обзира на тип, величину и природу организације (International Organization for Standardization, 2019).

Поред овог стандарда, у области континуитета пословања развијени су допунски стандарди из исте „породице стандарда”, који нису ни мање важни ни мање употребљиви, и који фокус стављају у првом случају на разраду основног стандарда, људски аспект континуитета пословања и примену на делатност управљања ланцем снабдевања (supply chain), а у другом случају на различите захтеве система управљања континуитетом пословања, као што су стратегије, планови и процедуре и анализа утицаја на пословање. Реч је о следећим стандардима<sup>8</sup>: *ISO 22313:2020 Societal security – Business continuity management systems – Guidance on the use of ISO 22301*; *ISO/TS 22330:2018 Security and resilience – Business continuity management systems – Guidelines for people aspects of business continuity*; *ISO/TS 22318:2021 Societal security – Business continuity management systems – Guidelines for supply chain continuity*; *ISO/TS 22331:2018 Security and resilience – Business continuity management systems – Guidelines for business continuity strategy*; *ISO/TS 22332:2021 Security and resilience – Business continuity management systems – Guidelines for developing business continuity plans and procedures*; *ISO/TS 22317:2021 Societal security – Business continuity management systems – Guidelines for business impact analysis (BIA)*.

У области информационе технологије постоји стандард *ISO/IEC 27031:2011 Information technology – Security techniques – Guidelines for information and communication technology readiness for business continuity*, који садржи концепте и принципе спремности информационих и комуникационих технологија (ИКТ) за континуитет пословања, усмерених на побољшање ИКТ спремности организације, а у циљу обезбеђивања континуитета пословања. У процесу је замена овог стандарда новим – *ISO/IEC WD 27031 Information technology – Cybersecurity – Information and communication technology readiness for business continuity*. Од значаја су и стандарди *ISO/IEC 27000:2018 Information technology – Security techniques – Information security management systems – Overview and vocabulary*, који континуитет пословања препознаје као фактор пресудан за успешну имплементацију система за управљање безбедношћу информација, као и стандард *ISO/IEC 27002:2013 Information technology – Security techniques – Code of practice for information security*

8 Свим стандардима из „ИСО породице” приступљено је са <https://www.iso.org/standards.html>.

*controls*, који садржи посебну област која се односи на континуитет пословања – *аспекти информационе безбедности управљања континуитетом пословања*.

Стандардизација у области континуитета пословања обухватила је и компетенције за ревизију и сертификацију система управљања континуитетом пословања стандардом *ISO/IEC TS 17021-6:2014(en) Conformity assessment – Requirements for bodies providing audit and certification of management systems – Part 6: Competence requirements for auditing and certification of business continuity management systems*.

Навођење стандарда који у целини или у неком свом делу покривају област управљања континуитетом пословања не завршава се са Међународном организацијом за стандардизацију (ИСО породица стандарда). Вреди навести документа попут: *PD 25111:2010: Business continuity management. Guidance on human aspects of business continuity* и *PD 25666:2010: Business continuity management. Guidance on exercising and testing for continuity and contingency programmes* – публикација Британске институције за стандардизацију (British Standards Institution); *Good Practice Guidelines (GPG)* – публикације „добре праксе” Института за континуитет пословања (Business Continuity Institute); *BSI-Standard 200-4: Business Continuity Management* – стандарда немачког Савезног бироа за информациону безбедност (Federal Office for Information Security), а који треба бити замењен стандардом *BSI-Standard 200-4: Business Continuity Management* (који се налази у другој фази коментарисања<sup>9</sup>) или *NFPA 1600: Standard on Continuity, Emergency, and Crisis Management* – универзалног стандарда Националне асоцијације за заштиту од пожара (National Fire Protection Association).

Стандард NFPA 1600 признат је од стране Националне комисије за терористичке нападе на Сједињене Државе као национални стандард приправности, и од стране Министарства за унутрашњу безбедност САД као стандард добровољног консензуса за спремност за ванредне ситуације (NFPA, n.d.). Поред наведеног, 2020. године, Влада Велике Британије је усвојила сет индивидуалних стандарда за одржање отпорности на локалном нивоу, који обухвата управљање континуитетом пословања – *National Resilience Standards for Local Resilience Forums* (Cabinet Office, 2020). Иако ови стандарди нису намењени за међународну примену, њихово усвајање представља значајан корак који је

<sup>9</sup> Податак је преузет дана 10.10.2022. године са линка: [https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/BSI-Standard-200-4-Business-Continuity-Management/bsi-standard-200-4\\_Business\\_Continuity\\_Management\\_node.html](https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/BSI-Standard-200-4-Business-Continuity-Management/bsi-standard-200-4_Business_Continuity_Management_node.html)

начињен у овој области, с обзиром на то да укључује највиша државна тела у доношење норматива у области управљања континуитетом пословања.

У Републици Србији у примени је стандард из ISO породице – *SRPS EN ISO 22301:2020 Bezbednost i otpornost – Sistemi menadžmenta kontinuitetom poslovanja – Zahtevi*. Имплементација овог стандарда није обавезна већ се препоручује и извршава ради постизања позитивних ефеката које његова имплементација има.

## Прописи на нивоу Европске уније

На нивоу Европске уније не постоји документ који свеобухватно уређује област континуитета пословања. Упркос томе, у једном од докумената прописује се начин на који се може обезбедити континуитет пословања, али само за специфичан случај смрти власника (Publications Office of the European Union, 2006).

Ипак, иако не свеобухватно, постоји неколико докумената које овде вреди поменути. То су документи који се могу означити као „легислатива и регулатива” и, изузев првог, односе се на банкарски и финансијски сектор. Реч је о документима попут *Council Directive 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection* (повезан са *The European Programme for Critical Infrastructure Protection (EPCIP)*); *Directive 2009/138/EC of the European Parliament and of the Council on the taking-up and pursuit of the business of Insurance and Reinsurance (Solvency II)*; *High-level principles for business continuity*; *The New Basel Capital Accord (Basel II)*; *Basel III: A global regulatory framework for more resilient banks and banking systems* (унапређен претходни документ) (BCM, 2016).

Последњи наведени документ саставни је део такозваног *Basel Framework*-а, који такође има додирних тачака са облашћу управљања континуитетом пословања уређујући одређена питања, попут разматрања планова опоравка од катастрофе и континуитета пословања у циљу процене њихове изводљивости у сценаријима озбиљног поремећаја пословања (Principle 25, BCP Core Principles for effective banking supervision, 2019) и разматрања података о ризицима и праксе извештавања о ризицима као део процеса планирања континуитета пословања и као предмета анализе утицаја на пословање (Principle 2, SRP

Supervisory review process, 2019). Треба имати у виду да су наведене две обавезе директно повезане са процесом којим се бавимо у овом раду, што не значи да не постоји још питања која овај скуп докумената на мање или више непосредан начин регулише, попут области управљања ризицима која је тесно повезана са континуитетом пословања.

Из наведеног се може закључити да је управљање континуитетом пословања обухваћено само у неким сегментима и то само за неке области попут критичне инфраструктуре и банкарског и финансијског сектора. Имајући то у виду, може се закључити, не улазећи у свеобухватну анализу конкретних одредби, да су се области у којима се ова функција мање или више разрађује исте у нашој држави и на нивоу Европске уније. Притом, не сме се испустити из вида чињеница да је фокус у раду стављен на прописе на нивоу Европске уније, не разматрајући појединачну регулативу земаља чланица, што оставља простора за даље анализе у том правцу.

## Закључак

Из приложеног текста, анализе различитих докумената са или без правне снаге указују на то да је области континуитета пословања посвећена пажња. Исправно би било рећи да обим те пажње варира од документа до документа и да се односи у неким случајевима на функцију државе, и у другим случајевима на организације у различитим индустријама. Држава је неупитни провајдер безбедности и свих осталих функција неопходних за постојање и континуиран рад њених елемената. Као таква, држава је дужна да обезбеди континуирано спровођење свих виталних функција, попут пружања основних јавних добара, одбране, реда и закона, здравствене, социјалне, образовне и друге. Анализирајући домаће позитивно законодавство, држава планира и припрема активности које би се спроводиле у свим оним ситуацијама у којима може доћи или је дошло до нарушавања једне или више функција за које је одговорна (ратно или ванредно стање) и, сходно томе, а преко својих органа, обезбеђује континуирано функционисање заједнице.

Ситуација на нивоу правних лица је нешто другачија. Генерално посматрано, на међународном нивоу, управљање континуитетом пословања је област која повезује експерте који имају за циљ развијање и

унапређење ове области. Уз то, данас постоји низ прописа – стандарда, „добрих пракси”, који садрже како теоријска знања тако и практична упутства и смернице за имплементацију и усавршавање управљања континуитетом пословања, односно система који се успоставља ради ове функције. Са друге стране, изузев у областима заштите критичне инфраструктуре и банкарског и финансијског пословања, законодавство не препознаје управљање континуитетом пословања као обавезну функцију, а самим тим је ни не уређује. Поставља се питање да ли је овакво (не)деловање државе оправдано?

Да ли држава треба да уреди ову област као што је уредила, на пример, област приватног обезбеђења, доневши закон који је поставио конкретне оквире области приватног обезбеђења 2013. године и уредио (бар већину) питања из ове области, укључујући, на пример, и обавезу израде акта о процени ризика, или треба да пусти да то тржиште уради? Истина је да је област приватног обезбеђења све значајнија, и то не само за приватни сектор, већ и за целокупни јавни сектор, у контексту извршавања задатака обезбеђења и доприноса укупној безбедности државе и друштва, те самим тим уплитање државе у њено регулисање јесте без премца.

Међутим, осврнимо се на област континуитета пословања. Континуитет пословања постоји и код јавних и код приватних ентитета, који су данас међузависни вероватно више него икада пре. Држава и њено функционисање у великој мери зависе од организација, или, конкретније, правних лица, и то не само оних који су препознати као критична инфраструктура. Дакле, правна лица не функционишу само за себе, већ својим добрим пословањем и резултатима рада индиректно доприносе и функционисању државе. То се нарочито односи на она, надовезујући се на претходно изнето, која су неопходна држави да континуирано функционише. Узимајући у обзир наведено, већа заинтересованост државе за питања континуитета пословања била би не само оправдана већ и пожељна.

Узмимо за пример пандемију са којом се свет и даље суочава, додуше, у мањој мери него када је иста проглашена услед енормних последица. Пандемија је пред свако правно лице поставила ризик по наставак функционисања, доводећи у реалистичко питање и сам њихов опстанак. Правна лица су се суочила са проблемима попут недостатка радне снаге, кашњења материјала, кашњења испоруке добара и услуга, тешкоћа у спровођењу радних активности, што је утицало на њихово пословање.

Поред тога што се директно суочава са пандемијом и њеним последицама, држава и индиректно „осећа” последице које погађају правна лица. Управо у циљу адекватније „борбе” против догађаја попут пандемија, оних догађаја за које није познато колико ће трајати и који ће бити свеукупни збир последица, држава треба да предузме кораке ка већој укључености у област континуитета пословања. На пример, уколико је држава могла да пропише обавезу израде, односно поседовања акта о процени ризика у заштити лица, имовине и пословања, позивајући се на релевантни стандард у тој области, могла би и да пропише обавезу израде, односно поседовања плана континуитета пословања такође се позивајући на релевантни стандард у тој области. Свакако, већа заинтересованост и укљученост државе у разматрању област само би могло да има позитивне ефекте како за правна лица тако и државну управу, службе и све организације и институције које регулишу друштвене процесе, доприносећи пословању на микро и макронивоу.

## ЛИТЕРАТУРА

- Basel Committee on Banking Supervision (2019). *SRP Supervisory review process*. Basel: Bank for International Settlements. Download [https://www.bis.org/basel\\_framework/chapter/SRP/10.htm](https://www.bis.org/basel_framework/chapter/SRP/10.htm)
- BCM Legislations, Regulations, Standards and Good Practice (2016). Berkshire: Business Continuity Institute. Download <https://www.thebci.org/static/uploaded/aa17d414-03ac-4ddb-a43657dd6297312d.pdf>
- BCP Core Principles for effective banking supervision (2019). Basel: Bank for International Settlements. Download <https://www.bis.org/publ/bcbs230.htm>
- Borodzicz, E. (2005). *Risk, Crisis and Security Management*. West Sussex: John Wiley & Sons.
- Bundesamt für Sicherheit in der Informationstechnik. (n.d.). *Modernisierter BSI-Standard 200-4 Business Continuity Management*. Accessed 10.10.2022; [https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/BSI-Standard-200-4-Business-Continuity-Management/bsi-standard-200-4\\_Business\\_Continuity\\_Management\\_node.html](https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/BSI-Standard-200-4-Business-Continuity-Management/bsi-standard-200-4_Business_Continuity_Management_node.html)
- Cabinet Office (2020). *National Resilience Standards for Local Resilience Forums (LRFs)*. Government UK. Downloaded <https://www.gov.uk/government/publications/national-resilience-standards-for-local-resilience-forums-lrfs>
- Cornish, M. (2010). Business Continuity Management Methodology. In A. Hiles (Ed.), *The Definitive Handbook of Business Continuity Management* (3rd ed.). West Sussex: John Wiley & Sons.

- Elliott, D. (2014). Disaster and Crisis Management. In M.Gill (ed.). *Handbook of Security* (2nd ed., pp. 813–836). London: Palgrave Macmillan.
- Federal Office for Information Security (2009). *BSI-Standard: 100-4 Business Continuity Management* (BSI Standard No. 100–4). Downloaded [https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard\\_100-4\\_e\\_pdf.html](https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-4_e_pdf.html)
- Gibb, F., & Buchanan, S. (2006). A framework for business continuity management. *International journal of information management*, 26(2), 128–141.
- Herbane, B. (2010). The evolution of business continuity management: A historical review of practices and drivers. *Business history*, 52(6), 978–1002.
- Herbane, B., Elliott, D., & Swartz, E. M. (2004). Business continuity management: time for a strategic role?. *Long range planning*, 37(5), 435–457.
- International Organization for Standardization (2019). *Security and resilience – Business continuity management systems – Requirements* (ISO Standard No. 22301:2019). Accessed <https://www.iso.org/obp/ui#iso:std:iso:22301:ed-2:v1:en>
- International Organization for Standardization. (n.d.). *Standards*. <https://www.iso.org/standards.html>
- Kovacich, L. G., & Halibozek, P. E. (2003). *The manager's handbook for corporate security: establishing and managing a successful assets protection program*. Burlington: Butterworth–Heinemann is an imprint of Elsevier Science.
- Мандић, Ј. Г., и Станојевић, П. (2020). *Корпоративна безбедност*. Београд: Факултет безбедности Универзитета у Београду.
- Милошевић, М. М. (2012). *Одговорност правних лица за кривична дела* (Докторска дисертација). Универзитет у Београду.
- National Fire Protection Association. (n.d.). *NFPA 1600. National Fire Protection Association*. Accessed 05.09.2022; <https://www.nfpa.org/codes-and-standards/all-codes-and-standards/list-of-codes-and-standards/detail?code=1600>
- Publications Office of the European Union (2006). (COM (2006) 117 final): *Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions – Implementing the Lisbon Community Programme for Growth and Jobs – Transfer of Businesses – Continuity through a new beginning*; <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52006DC0117&qid=1643126334789>
- Randeree, K., Mahal, A., & Narwani, A. (2012). A business continuity management maturity model for the UAE banking sector. *Business Process Management Journal*, 18(3), 472–492.
- Smith, L. C., & Brooks, J. D. (2013). *Security Science: The Theory and Practice of Security*. Waltham: Butterworth-Heinemann is an imprint of Elsevier.
- Speight, P. (2011). Business Continuity. *Journal of Applied Security Research*, 6(4), 529–554.

### Правни извори Републике Србије

- Доктрина Војске Србије (2010). Медија центар „Одбрана”, Београд.
- Закон о банкама (2005). „Сл. гласник РС”, бр. 107/2005, 91/2010 и 14/2015.

- Закон о информационој безбедности* (2016). „Сл. гласник РС”, бр. 6/2016, 94/2017, 77/2019.
- Закон о критичној инфраструктури* (2018). „Сл. гласник РС”, бр. 87/2018.
- Закон о одбрани.* (2007). „Сл. гласник РС”, бр. 116/2007, 88/2009, 88/2009 – др. закон, 104/2009 – др. закон, 10/2015 и 36/2018.
- Закон о приватном обезбеђењу* (2013). „Службени гласник РС”, бр. 104/2013, 42/2015, 87/2018.
- Закон о привредним друштвима* (2011). „Сл. гласник РС”, бр. 36/2011, 99/2011, 83/2014 (др. закон), 5/2015-3, 44/2018, 95/2018, 91/2019, 109/2021.
- Закон о смањењу ризика од катастрофа и управљању ванредним ситуацијама* (2018). „Службени гласник РС”, број 87/2018.
- Одлука о минималним стандардима управљања информационом системом финансијске институције* (2013). „Службени гласник РС”, бр. 23/2013, 113/2013, 2/2017, 88/2019, 37/2021.
- Одлука о одређивању правних лица од значаја за одбрану Републике Србије* (2008). „Сл. гласник РС”, бр. 52/2008.
- Одлука о плановима опоравка банке и банкарске групе* (2015). „Службени гласник РС”, бр. 71/2015.
- Одлука о управљању ризицима банке* (2011). „Службени гласник РС”, бр. 45/2011, 94/2011, 119/2012, 123/2012, 23/2013 (др. одлука), 43/2013, 92/2013, 33/2015, 61/2015, 61/2016, 103/2016, 119/2017, 76/2018, 57/2019, 88/2019, 27/2020, 67/2020 (др. одлука).
- Правилник о начину израде и садржају Плана заштите од пожара аутономне покрајине, јединице локалне самоуправе и субјеката разврстаних у прву и другу категорију* (2010). „Сл. гласник РС”, бр. 73/2010.
- Правилник о начину обављања појединачних полицијских послова* (2018). „Сл. гласник РС”, бр. 63/2018 и 72/2018.
- Стратегија националне безбедности Републике Србије* (2019). „Сл. гласник РС”, бр. 94/2009.
- Стратегија одбране Републике Србије* (2019). „Сл. гласник РС”, бр. 94/2019.
- Стратегија развоја Министарства унутрашњих послова за период 2018–2023. године* (2018). „Сл. гласник РС”, бр. 78/2018.
- Уредба о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја* (2016). „Сл. гласник РС”, бр. 94/2016.
- Уредба о начину и поступку извршавања обавезе планирања припрема за одбрану* (2009). „Сл. гласник РС”, бр. 24/2009.

## **NORMATIVE REGULATION OF BUSINESS CONTINUITY MANAGEMENT IN THE REPUBLIC OF SERBIA**

MA Jana Marković, PhD Student  
*University of Belgrade, Faculty of Security Studies*

### ***Summary***

The problem addressed in this paper concerns business continuity, that is, business continuity management. Business continuity management can be understood as one of the basic functions of any organization, the establishment and realization of which is necessary to ensure the continuation of business and at the same time the functioning of the organization in the event of any disruption caused by a potentially harmful event. On the other hand, it is not wrong to understand this function as an integral part of corporate security. This paper started from the research question of whether there is an adequate normative framework for business continuity management in the Republic of Serbia. In the paper, the author researched whether the business continuity management process is normatively regulated in a satisfactory manner, specifically, the legal regulations of the Republic of Serbia, standards in this area, but also regulations at the level of the European Union, in order to determine the relevant provisions that are missing in the legislation of the Republic of Serbia. The expected result is that, on the basis of a comprehensive analysis of the content of the documents that regulate business continuity management for the Republic of Serbia, and then on a level that goes beyond the borders of the state – for the international community in the field of business continuity created by state and non-state entities that aim to have a more comprehensive understanding and applying the business continuity concept. The author uses everything presented so far in order to point out the normative regulation of the subject area in the Republic of Serbia, but also more broadly, the importance of the entire area of business continuity, as well as the importance of greater involvement of the state in the regulation of issues of this type.

**Keywords:** *organizational function, business continuity management, legal regulations, standards.*