

Goran J. Mandić\*  
Nenad Putnik\*\*  
Sandra Rakic\*\*\*

UDK 005.332:[616.98:578.834  
005.334:334.72  
005.961:005.81  
DOI: 10.5937/MegRev2104025M  
Stručni članak  
Primljen 16.06.2021.  
Odobren 17.08.2021.

## KONTINUITET POSLOVANJA KAO FUNKCIJA KORPORATIVNE BEZBEDNOSTI – STUDIJA SLUČAJA PANDEMIJA SARS-CoV 2

**Sažetak:** *Kontinuitet poslovanja zauzima važno mesto kako u akademskoj sferi tako i u praktičnoj primeni koja se sprovodi u cilju obezbeđivanja funkcionalnosti pravnog lica. Mnogostruko složeni faktori i pretnje koji oblikuju ne samo nacionalnu već i globalnu bezbednost, značajno utiču na funkcionisanje korporacija što čini tradicionalni pristup korporativnoj bezbednosti relativno zastarelim. Cilj ovog članka je da prikaže najznačajnije diskusije u vezi sa ovim fenomenom u okviru akademske literature, kao i da identifikuje pitanja koja su od važnosti za uspešnu teorijsku nadgradnju i primenu ovog koncepta u praksi poslovanja. Autori razmatraju koncept kontinuiteta poslovanja kao jedan od značajnijih koncepata u funkciji korporativne bezbednosti, imajući u vidu izazove i pretnje sa kojima se suočavaju kompanije, a naročito one koje svoje poslovanje orijentišu ka izvozu ka inostranim tržištima. Pandemija izazvana virusom SARS - CoV 2, koja je kulminirala tokom 2020. godine, umnogome je pokazala slabosti „klasičnog“ planiranja kontinuiteta poslovanja imajući u vidu da su brojne kompanije u Srbiji, ali i u svetu obustavile u potpunosti svoje proizvodne procese. Zbog toga će u ovom radu na primeru pandemije delom biti identifikovane dosadašnje slabosti, kao i preporuke kojima bi se osigurao kontinuitet radnog procesa i time ostvarila funkcionalnost korporacija.*

**Ključne reči:** *korporativna bezbednost, korporacija, kontinuitet poslovanja, upravljanje rizicima, SARS - CoV 2*

---

\* Fakultet bezbednosti Univerziteta u Beogradu; goran.mandic@fb.bg.ac.rs

\*\* Fakultet bezbednosti Univerziteta u Beogradu; nputnik@fb.bg.ac.rs

\*\*\* Fakultet za preduzetnički biznis i menadžment nekretnina Univerziteta Union Nikola Tesla; sandrarakic@yahoo.com

## 1. Uvod

Problematizacija određenja korporativne bezbednosti je u kombinaciji sa novim pristupom kontinuiteta poslovanja, verovatno jedno od najznačajnijih polja koje se analizira u okviru akademske zajednice. Paralelan tok dva procesa – usložnjavanja i povećanja obima činilaca koji potpadaju pod „korporativnu zaštitu“ kao štice vrednosti sa jedne i inoviranje paradigme kontinuiteta poslovanja sa druge strane, čine ovaj problem još složenijim. Potreba za nesmetanim organizovanjem procesa poslovanja proističe iz želje za profitom, ali i nesmetanim pružanjem proizvoda i usluga redovnim korisnicima zarad očuvanja poslovnog ugleda kompanija. Zbog toga krize, naročito one koje nastupaju iznenada i koje ostavljaju posledice po funkcionisanje kompanija, predstavljaju glavni izazov u nesmetanom poslovanju. Dodatno, sa razvojem međunarodnopolitičkih tokova koji utiču naročito na transnacionalne kompanije, kao i napretkom tehnoloških dostignuća u svim aspektima života, pretnje i moguće neželjene krize usložnjavaju napore za „odbranom“ proizvodnih i poslovnih procesa kompanija širom sveta. Jedan od najsvežijih takvih *sui generis* primera je upravo pandemija izazvana virusom SARS - CoV 2, koja se dogodila tokom 2020. godine, a od koje se globalna privreda još uvek oporavlja. Pandemija je po ko zna koji put aktualizovala pitanje kontinuiteta poslovnog procesa, promovišući ovu funkciju visoko na agendi korporativne bezbednosti.

Ne samo da je pandemija poslužila pojedinim političkim elitama da promovišu svoje autoritarne prakse što je bio primer u slučaju Turkmenistana ili Mađarske, već je mnogo značajnije pitanje koje je nastalo kao posledica pandemije - ekonomsko regulisanje tržišta, zatvaranje kompanija, opstanka i stabilnosti čitavih grana poslova, kao i uticaja veštačkog stimulisanja ekonomija od strane svake države na stabilnost poslova i opstanak kompanija<sup>1</sup>. Ova pandemija je pokazala da je globalno društvo bilo nespremno da na najbazičnijem nivou odgovori na izazove velikih razmera. Dodatno, otvorenost država i trgovinska međuzavisnost uslovile su dodatne probleme i komplikacije u snabdevanju na globalnom nivou, što je ponovo uticalo na kontinuitet i stabilnost poslovanja mnogih kompanija<sup>2</sup>. Često prenebreavana funkcija korporativne bezbednosti – fizička zaštita imovine, kao i opstanak kompanije na tržištu, nažalost je ispoljena tokom prethodne godine u najdirektnijoj formi. Zbog toga je važno predstaviti tok akademske diskusije koja se u prethodnim godinama razvijala u vezi sa kontinuitetom poslovanja kao garantom opstanka kompanija, naročito u uslovima katastrofalnih kriza.

Zbog toga je primer pandemije SARS - CoV 2 podesan analitički alat u sveobuhvatnijem sagledavanju funkcionisanja kompanija i zabrinutosti o nesmetanom poslovnom procesu. Akademski radovi u domaćoj naučnoj literaturi nisu

<sup>1</sup> Donthu, N., Gustafsson, A. (2020): Effects of COVID-19 on business and research. Journal of business research, 117, 284-289.

<sup>2</sup> Ibid.

tokom prethodne godine posvećivali značajniju pažnju posledicama pandemije na poslovanje korporacija i na stabilnost njihovih poslovnih procesa. Iz tog razloga, ovaj rad predstavlja svojevrsni pokušaj sistematizacije naučne građe pre početka krize, a što je od značaja za primenu takvih (sa)znanja na analiziranje uticaja i posledica pandemije na korporativnu bezbednost.

Na početku rada predstavljeni su različiti pristupi operacionalizaciji pojma korporativne bezbednosti, kao i njene glavne dimenzije i funkcije. Zbog usložnjavanja proizvodnih procesa i udela koji digitalizacija mnogih poslova ima u odnosu na prethodne decenije, autori identifikuju elemente inoviranja paradigme korporativne bezbednosti. Zatim se prikazuje kontinuitet poslovanja u smislu njegove uloge koju ostvaruje kao funkcija korporativne bezbednosti. Autori razmatraju krizne situacije koje predstavljaju izazov po kontinuitet poslovanja kroz studiju slučaja aktuelne pandemije izazvane virusom SARS - CoV 2. U ovom delu rada predstavljeni su nalazi dosadašnjih istraživanja koji ukazuju na promene u navikama potrošača, načine na koje bi kompanije trebalo da orijentišu svoje planove za kontinuitet poslovanja, zatim modalitete prilagođavanja na krizne situacije slične pandemiji, kao i vrste inovacija na koje bi kompanije trebalo da se oslone u svom budućem poslovanju. Na kraju, autori sumiraju najznačajnija pitanja koja pomažu teorijskoj nadgradnji i primeni koncepta u praksi koja će u budućnosti biti oblikovana još kompleksnijim izazovima po korporativnu bezbednost.

## **2. Osavremenjivanje paradigme korporativne bezbednosti**

U klasičnom definisanju pojma korporativne bezbednosti polazi se od potrebe pravnog lica za osiguranjem poslovnog procesa, kao i imovine i zaštite lica koja učestvuju u proizvodnom procesu. Korporativna bezbednost se često, mada pogrešno, tretira kao korporativni trošak, a ne kao vrednost koja svojim postojanjem doprinosi povećanju profita kompanijama<sup>3</sup>. Lipert i saradnici navode da se korporativna bezbednost poistovećuje sa ostalim troškovima poput službenih putovanja, računara i opreme i slično, što u uslovima ekonomske krize za posledicu ima gašenje čitavih odeljenja koja bi se trebalo baviti ovom problematikom<sup>4</sup>. U svom članku iz 2013. godine, Lipert i saradnici su tvrdili da je „došlo vreme za sveobuhvatniju raspravu“ u vezi sa novim tipologijama korporativne bezbednosti. Oni veruju da je svrha ovog zadatka „olakšavanje produbljene analize, povećanje nivoa razumevanja i pokretanje širih pitanja na društvenom i političkom planu“<sup>5</sup>. S tim u vezi, prva promena odnosi se na razlikovanje pojedinih sličnih konceptata koji su predstavljeni u akademskim radovima. Tako, na

<sup>3</sup> Lippert, K., Walby, K., Steckle, R. (2013): Multiplicities of corporate security: Identifying emerging types, trends and issues. *Security Journal*, 26(3), 206-221.

<sup>4</sup> Ibid.

<sup>5</sup> Ibid.

primer, Džejs Vilijams (*James Williams*) navodi da je srodan termin "privatna bezbednost" prevaziđen upravo zbog usložnjavanja procesa i „složenosti tipologije korporativne bezbednosti“<sup>6</sup>.

Takve tipologije proizilaze iz novih izvora pretnji koje nisu više jednoznačne. Odgovor na tradicionalne pretnje poput prirodnih (požari, poplave, zemljotresi, olujni vetrovi) i onih uzrokovanih ljudskim faktorima više nije dovoljan u očuvanju korporativne bezbednosti<sup>7</sup>. U novoj tipologiji pretnji po bezbednost poslovanja izdvajaju se pandemije, nepouzdana podaci, narušavanje funkcionisanja softvera i hardvera, kao i svi izazovi koji proističu iz razvoja globalnog interneta<sup>8</sup>. Pojedini autori, čak, uključuju kontinuitet poslovanja i korporativnu bezbednost kao značajne faktore u klasičnim oružanim sukobima, naročito ako su u pitanju kompanije koje se bave vojnim konsultantskim uslugama ili proizvodnjom vojne opreme i oružja<sup>9</sup>. Drugi autori su ustanovili da je promena hazarda koji svojim ispoljavanjem mogu da naruše poslovni proces kompanija, veoma brzo promenila svoju fizionomiju<sup>10</sup>. Naime, krajem XX veka, najveći procenat pretnji po korporacije dolazio je od fizičkog ugrožavanja imovine, proizvodnih pogona i prostorija kompanija od strane prirodnih nepogoda, zemljotresa ili cunamija. To je u najvećoj meri i opterećivalo kompanije i planove kontinuiteta poslovanja, imajući u vidu da se na ispoljavanje ovih fenomena ni na koji način ne može uticati, osim u domenu odgovora nakon njihovog ispoljavanja. Međutim, na kraju prve decenije XXI veka fenomenologija ovih pretnji je promenjena, tako da je udeo prirodnih nepogoda najniži, zatim ga prate izazovi koji se odnose na dislociranje proizvodnih pogona i/ili procesa i usluga, i na kraju greške i prepreke koje proizilaze iz neadekvatnog rukovanja hardverom. Zbog toga ovaj autorski tim predviđa da će u budućnosti biti potpuno izražena dominacija softverskih grešaka prilikom funkcionisanja poslovnih procesa, jer će se oni u najvećoj meri oslanjati na digitalizaciju usluga<sup>11</sup>. Važno je napomenuti da navedeni autori među moguće pretnjame po korporativnu bezbednost svrstavaju i ljudske greške, nedostatak snabdevanja električnom energijom, greške u komunikaciji, kao i nesporazume sa pružiocima usluga i primarnih sirovina neophodnih za proizvodnju<sup>12</sup>.

<sup>6</sup> Williams, J. (2005): Reflections on the private versus public policing of economic crime. *The British Journal of Criminology*, 45(3), 316–339.

<sup>7</sup> Halibozek, E., Kovacich, G. (2017): *The manager's handbook for corporate security: establishing and managing a successful assets protection program*. Butterworth-Heinemann.

<sup>8</sup> Botha, J., Von Solms, R. (2004): A cyclic approach to business continuity planning. *Information Management & Computer Security*, 12(4), 328-337.

<sup>9</sup> Wolf, K., Deitelhoff, N., Engert, S. (2007): Corporate security responsibility: Towards a conceptual framework for a comparative research agenda. *Cooperation and Conflict*, 42(3), 294-320.

<sup>10</sup> Cerullo, V., Cerullo, M. (2004): Business continuity planning: a comprehensive approach. *Information systems management*, 21, 70-78.

<sup>11</sup> Ibid, str. 73.

<sup>12</sup> Cerullo, V., Cerullo, M. (2004): Business continuity planning: a comprehensive approach. *Information systems management*, 21, 70-78.

Klaus Volf (*Klauss Wolf*) i saradnici navode da u međunarodnom domenu, korporativna bezbednost, preciznije, korporacije ostvaruju specifičnu „bezbednosnu korporativnu odgovornost“ u nastojanju da okončaju oružane sukobe ili sačuvaju mir<sup>13</sup>. Prema ovakvom viđenju, takva korporativna „odgovornost“ bazirana je na pretpostavci o „humanizaciji rata“ i spasavanju velikog broja civilih (ali i vojnih) žrtava upotrebom savremenih tehnoloških rešenja koja menjaju fizionomiju ratovanja<sup>14</sup>. Još jedno od autentičnih objašnjenja inoviranja korporativne bezbednosti nalazi se u radu Karena Peteresena (*Karen Petersen*). On smešta menadžera za korporativnu bezbednost u područje između nacionalne i korporativne bezbednosti, označavajući ga terminom „hibridni posrednik“<sup>15</sup>. Interesantan je statistički podatak da su prethodna zanimanja *bezbednosnih menadžera* bila iz sfere policijskih poslova (oko 31%), zatim obaveštajni sektor (oko 19%), oružane snage (21%) i ostali oko 30%<sup>16</sup>.

Petersen ukazuje na profesionalizaciju zanimanja *menadžera bezbednosti* koja je nastala kao posledica usloženjenih procesa i novih pretnji po bezbednost ne samo na nacionalnom, nego i na međunarodnom nivou<sup>17</sup>. Stoga je nesumnjivo da korporativna bezbednost predstavlja širi pojam u odnosu na pojam kontinuiteta poslovanja budući da kontinuitet poslovnog procesa predstavlja samo jednu od funkcija i dimenzija bezbednosti poslovanja.

Zbog toga i ne čudi pluralitet identifikovanih pravaca i nedoslednosti u literaturi kada je ova tema u pitanju, kao ni u praksi, gde je prisutan problem loše obuke osoblja za fizičko obezbeđenje objekata<sup>18</sup> ili angažovanih službi obezbeđenja korporacija, odnosno službi obezbeđenja. S tim u vezi, u naučnoj i stručnoj literaturi se javlja zanimljivo segmentiranje korporativne bezbednosti na nekoliko dimenzija. Opisujući takozvanu tipologiju korporativne bezbednosti, Lipert i saradnici je razlažu na pet segmenata. Prema njihovom stanovištu, ona obuhvata: utvrđivanje vlasništva (privatno/državno) nad kompanijom ili proizvodnim procesom; način na koji je organizovan poslovni i radni proces; nadgledanje rada kako zaposlenih tako i celokupnog procesa; nadzor nad službom fizičkog obezbeđenja i, način selekcije i obuke kadra koji je zadužen za bezbednost<sup>19</sup>.

<sup>13</sup> Wolf, K., Deitelhoff, N., Engert, S. (2007): Corporate security responsibility: Towards a conceptual framework for a comparative research agenda. *Cooperation and Conflict*, 42(3), 294-320, str. 298.

<sup>14</sup> Ibid, str. 298-299.

<sup>15</sup> Petersen, K. (2013): The corporate security professional: A hybrid agent between corporate and national security. *Security journal*, 26(3), 222-235, str. 7.

<sup>16</sup> Briggs, R., Edwards, C. (2006): *The business of Resilience: Corporate Security for the 21th Century*. London: Demos, str. 79.

<sup>17</sup> Petersen, K. (2013): The corporate security professional: A hybrid agent between corporate and national security. *Security journal*, 26(3), 222-235.

<sup>18</sup> Lippert, K., Walby, K., Steckle, R. (2013): Multiplicities of corporate security: Identifying emerging types, trends and issues. *Security Journal*, 26(3), 206-221.

<sup>19</sup> Ibid.

Lipert i saradnici veruju da svaka od navedenih dimenzija umnogome doprinosi načinu na koji se analitički posmatra korporativna bezbednost što posledično dovodi do poboljšanja njenog nivoa.

Paradigma korporativne bezbednosti je nesumnjivo inovirana delovanjem faktora koji utiču na sveukupnu promenu globalnog okruženja. Korporacije odavno više ne brinu samo o bezbednosti imovine i svojih zaposlenih na radnom mestu, već o mnogo širem spektru izazova koji stoje pred njima. Ovakav stav zastupaju Rejčel Brigs (*Rachel Briggs*) i Čarli Edvards (*Charlie Edwards*). Klasično narušavanje nacionalne i međunarodne bezbednosti nekonvencionalnim sredstvima u kojima ciljevi napada više nisu isključivo vojni objekti, u velikoj meri ugrožava poslovanje kompanija. U prilog ovoj tvrdnji oni navode uticaj efikasnog upravljanja bezbednošću poslovanja u uslovima „inovirane bezbednosne paradigme“ na benefite koje ostvaruju korporacije - u prvoj instanci na profit. U anketi u kojoj su učestvovali izvršni menadžeri i direktori najvećih svetskih kompanija, najviše njih se izjasnilo da je kontinuitet poslovanja i procesa proizvodnje najvažniji za profit kompanije – čak 80% ispitanih. Daleko ispod toga nalaze se zaštita brenda i ugleda kompanije, zatim očuvanje poverenja akcionara i suvlasnika, kao i povoljno upravljanje kadrovima<sup>20</sup>. Zanimljivo je da je ova anketa pokazala da je svega 44% ispitanika smatralo da je očuvanje prava intelektualne svojine i kapaciteta za regrutovanje velikog broja kvalitetnog kadra, važno za profit u uslovima novih bezbednosnih rizika i pretnji na globalnom planu<sup>21</sup>.

Iz prethodnih razmatranja jasno proističe stav da je korporativnu bezbednost potrebno sagledavati kao kvalitativno novu vrednost u odnosu na klasično posmatranu sigurnost poslovanja, imovine i lica koja su angažovana u radnom procesu, a kontinuitet poslovanja kao jednu od značajnijih funkcija korporativne bezbednosti koja se odnosi na efikasno upravljanje kriznim situacijama.

### 3. Kontinuitet poslovanja kao funkcija korporativne bezbednosti

U literaturi je koncept kontinuiteta poslovanja vezan za upravljačku dimenziju, pa se često govori o „menadžmentu kontinuiteta poslovanja“, odnosno upravljanju kontinuitetom poslovnog procesa (*Business Continuity Management – BCM*). Kovačić i Hejlbozek navode čak dvanaest funkcija korporativne bezbednosti, među kojima je i planiranje kontinuiteta poslovanja. Osim planiranja kontinuiteta poslovanja među funkcije korporativne bezbednosti svrstane su: bezbednost oličena kroz administrativno upravljanje, fizička sigurnost, lična bezbednost, regulisanje „vlasništva“ nad službom fizičkog obezbeđenja, obrazovanje i obuka u sferi bezbednosti, zaštita od požara, unutrašnje istrage, bezbed-

<sup>20</sup> Briggs, R., Edwards, C. (2006): *The business of Resilience: Corporate Security for the 21st Century*. London: Demos, str. 27.

<sup>21</sup> Ibid, str 27.

nost informacija, zaštita izvršnih direktora i menadžmenta korporacija i bezbednost događaja<sup>22</sup>. Prema ovoj klasifikaciji, kontinuitet poslovanja je sastavni deo „korporativne politike bezbednosti“ i treba da se razvija u okviru odeljenja za planiranje u korporacijama u okviru kojih je potrebno razviti „Program kontinuiteta planiranja“<sup>23</sup>. Takav program, treba da se konkretizuje međusobnom interakcijom tri segmenta: odgovor na krize i vanredne situacije, upravljanje kriznim situacijama, i kontinuitetom poslovanja<sup>24</sup>. Oni vrše jasnu distinkciju između termina kontinuitet poslovanja (*business continuity*), neočekivana kriza (*contingency*) i planiranje za neočekivane krizne situacije (*contingency planning*). Među kriterijume i termine koji su od analitičkog značaja za korporativnu bezbednost, oni svrstavaju i inicijalni oporavak poslovanja koji se odnosi na povratak aktivnosti na prethodno stanje u roku kraćem od 60 dana od nastupanja katastrofa ili kriznih situacija, dok nastavak poslovanja (*business resumption*) ovi autori tretiraju kao dugoročniji proces povraćaja svih poslovnih aktivnosti u periodu dužem od dva meseca nakon kriza<sup>25</sup>.

Kontinuitet poslovanja navedeni autori definišu kao „miminizovanje obustavljanja poslovnog procesa uslovljenog iznenadnim događajima i krizama“, zbog čega dobri planovi za nastavak poslovanja obuhvataju sve mere upravljanja i aktivnosti koje poboljšavaju ovaj proces<sup>26</sup>. Svoju tvrdnju o planovima za kontinuirano poslovanje, oni razrađuju definicijom planiranja za neočekivane krize. Njome obuhvataju sve planove koji predviđaju mere odgovora, oporavka, kao i nastavka aktivnosti poslovanja u vezi sa infrastrukturom (imovinom korporacija), vitalnim proizvodnim ili uslužnim procesima i ostalim elementima koji su imanentni specifičnostima neočekivanih kriza<sup>27</sup>. Konačno, kritičnim procesima ovi autori identifikuju sve procese koji su od vitalnog značaja za nesmetano funkcionisanje kompanije ili poslovnog procesa, a čije narušavanje ima za posledicu nemogućnost sticanja profita, ispunjavanje ugovorne obaveze ili druge pravne konsekvence<sup>28</sup>. Ideja takozvanog „Programa za kontinuitet poslovanja“, prema ovim autorima, ogleda se u višestapnom planiranju koje uključuje mere koje se odnose na obezbeđivanje samog mesta proizvodnog procesa, koje u sebe uključuje efikasno komuniciranje, jasnu odgovornost svih zaposlenih, edukaciju zaposlenih i usmeravanje na bezbednost zaposlenih. Druga etapa planiranja sastoji se od plana za upravljanje krizom na konkretnom mestu koje uključuje

<sup>22</sup> Halibožek, E., Kovacich, G. (2017): *The manager's handbook for corporate security: establishing and managing a successful assets protection program*. Butterworth-Heinemann.

<sup>23</sup> Ibid, str. 287.

<sup>24</sup> Ibid, str. 288.

<sup>25</sup> Halibožek, E., Kovacich, G. (2017): *The manager's handbook for corporate security: establishing and managing a successful assets protection program*. Butterworth-Heinemann.

<sup>26</sup> Ibid, str. 289.

<sup>27</sup> Ibid, str. 290.

<sup>28</sup> Ibid, str. 290.

početnu procenu štete nakon krize, mere i aktivnosti za tranziciju kao i obaveštavanje o preduzetim merama. Poslednja etapa programa za kontinuitet poslovanja tiče se oporavka poslovnog procesa nakon što je nastupila kriza i obuhvata upravljanje i analize koje su usmerene na poslovni profit kao i na identifikovanje kritičnih procesa po nastavak poslovanja<sup>29</sup>.

Virdžinija i Majkl Cerulo (*Virginia Cerullo & Michael Cerullo*) tvrde da kontinuitet poslovanja treba da zadovolji tri specifična cilja koja su uzajamno zavisna. Najpre, dobar proces planiranja kontinuiteta poslovanja mora da identifikuje rizike koji mogu da naruše poslovni proces<sup>30</sup>. Zatim, ovaj proces mora da uključi plan za upravljanje rizicima ili pak za smanjivanje njihovih posledica. Na kraju, treći cilj planiranja kontinuiteta poslovanja mora da obuhvati i obuku zaposlenih i proveru efikasnosti samog plana<sup>31</sup>. Slično ostalim autorima, oni su ispitivali na koji način je promenjena paradigma u uključivanju informacione bezbednosti i kontinuiteta poslovanja u takozvanu *bezbednosnu funkciju poslovanja* kako je ovi autori nazivaju. Oni veruju da na informacionu i poslovnu bezbednost utiču pored eksternih i unutrašnji faktori koji se odnose na nedovoljno izgrađeno poverenje među zaposlenima i često nepoverenje zaposlenih u menadžment kompanije koji pravi planove za delovanje u kriznim situacijama<sup>32</sup>.

Rigs i Edwards su upravo na tragu ovog argumenta prepoznali nekoliko specifičnosti takozvanog "pomirenja" između biznisa i bezbednosti. Oni navode da odeljenja za planiranje kontinuiteta poslovanja treba da budu promovisana unutar kompanija kao poželjni organizacioni elementi koji doprinose profitu a ne kao "prisila nad radnicima"<sup>33</sup>. Osim toga, u uslovima kriznih situacija, bezbednost treba shvatiti kao pomoć kompaniji u odgovoru na rizike, zbog čega bezbednost (u najširem smislu) predstavlja izuzetno važnu komponentu planiranja kontinuiteta poslovanja<sup>34</sup>. Oni navode da je korporativna bezbednost, entitet koji valja istovremeno realizovati i na strateškom i na operativnom planu, ali da svi zaposleni i organizacione jedinice u svom domenu moraju da prave jasnu razliku između ove dva nivoa, naročito u slučaju kriza većeg obima<sup>35</sup>. Zbog toga rukovodioci sektora bezbednosti moraju da usade organizacionu kulturu zaposlenima zarad kompletne saradnje na poslovima obezbeđivanja poslovnog procesa i ujedno opstanka kompanije na tržištu<sup>36</sup>.

<sup>29</sup> Ibid, str. 291.

<sup>30</sup> Cerullo, V., Cerullo, M. (2004): Business continuity planning: a comprehensive approach. Information systems management, 21, 70-78, str. 71.

<sup>31</sup> Ibid, str. 71.

<sup>32</sup> Ibid, str. 76.

<sup>33</sup> Briggs, R., Edwards, C. (2006): The business of Resilience: Corporate Security for the 21th Century. London: Demos, str. 96.

<sup>34</sup> Ibid.

<sup>35</sup> Ibid, str. 97.

<sup>36</sup> Ibid, str. 99.

U literaturi se kao značajan faktor analizira i veličina preduzeća, budući da je upravljanje kontinuitetom poslovanja u značajnoj meri zavisno i od vrste i broja zaposlenih. Tako pojedini autori ukazuju da je za velika preduzeća i korporacije neophodno sprovesti takozvani „ciklični pristup“ u planiranju kontinuiteta poslovanja koji bi se sastojao iz nekoliko delova: planiranja, analize uticaja na poslovni proces, uključivanje ostalih strategija kontinuiteta poslovanja, edukacije, testiranja i održavanja ažurnim plana kontinuiteta poslovanja<sup>37</sup>. Jedno od važnih pitanja u vezi sa kontinuitetom poslovnog procesa, odnosi se na kvalitet života zaposlenih, kao posledicu adekvatnog upravljanja kontinuitetom poslovanja<sup>38</sup>. Ovi autori upućuju na šest polja na kojima se bazira kvalitet života: zaposlenost, ekonomski resursi, porodica, zdravlje, društvena uloga i obrazovanje/nauka<sup>39</sup>. Razmatrajući pitanje kvaliteta života, Arsovski i Milićević se ne ograničavaju samo na zaposlene, već i na širu društvenu zajednicu koja napreduje usled poboljšanja životnih uslova. Zbog toga oni u analizu planiranja poslovanja svake kompanije uključuju još tri indikatora koji značajno poboljšavaju kvalitet radnog procesa: kvalitet vremena (efektivno korišćenje radnog vremena za druge aktivnosti zaposlenih), zatim tzv. „kvalitativnost“ koja nastaje kao mešavina produktivnosti i kvaliteta, kao i kvalitet radnog života poput BZR, mogućnosti napretka u poslovnom smislu, razvoj kritičkog duha među zaposlenima i slično<sup>40</sup>. Slična istraživanja i teorijska proširenja upravljanjem kontinuiteta poslovanja u elektronskoj sferi (tzv. „eBCM - *electronic Business Continuity Management*“) sprovedena su i od strane drugih domaćih autora<sup>41</sup>. U elektronskoj sferi je naročito očigledno povećanje količine podataka sa kojima raspolaze kompanije, u zavisnosti od vrste i obima posla, tako da osobe koje rade na pozicijama planiranja kontinuiteta poslovanja, moraju da prate ovakve dinamične promene i da stalno prilagođavaju „odbrambene kapacitete“ za neželjene krize.

#### 4. Krizne situacije i kontinuiteta poslovanja – studija slučaja SARS - CoV 2

Kontinuitet poslovanja je ugrožen mnogostrukim faktorima koji se odnose na stabilnost i održivost poslovnog procesa. Jedan od centralnih faktora koji ugrožavaju poslovni proces jesu krizne situacije koje upućuju na potrebu za trenutnim reagovanjem, ali istovremeno ostavljaju i brojne posledice na dugoroč-

<sup>37</sup> Botha, J., Von Solms, R. (2004): A cyclic approach to business continuity planning. *Information Management & Computer Security*, 12(4), 328-337.

<sup>38</sup> Арсовски, С., Милићевећ, Р. (2010): «Менаџмент континуитетом пословања и квалитет живота.» Рад презентован на Фестивалу квалитета – 5. национална конференција о квалитету живота. Крагујевац: Факултет инжењерских наука.

<sup>39</sup> Ibid, str. 4.

<sup>40</sup> Ibid, str. 3.

<sup>41</sup> Лабус, М. (2020): Модел адаптивног управљања континуитетом електронског пословања. Београд: Универзитет у Београду-Факултет организационих наука.

nom planu. Pandemija izazvana virusom SARS - CoV 2 je ostavila dalekosežne posledice na globalnom nivou ne samo po zdravlje ljudi, već i na celokupno funkcionisanje privrednog sistema. Na kraju prvog talasa pandemije izazvane virusom SARS - CoV 2 (maj 2020), na globalnom nivou je čak 26% mikro, malih i srednjih preduzeća u potpunosti obustavilo svoj proizvodni proces, a podaci Svetske banke ukazuju da je tada najpogođeniji sektor bio turizam (sa preko 54% zatvorenih preduzeća), obrazovanje (47%) i ugostiteljstvo koje obuhvata hotele, kafiće i restorane (sa oko 32%)<sup>42</sup>.

Uticaj pandemije na kontinuitet poslovanja elaboriran je u većem broju akademskih radova u kojima su identifikovani i predstavljeni ključni izazovi za kompanije, prepoznati u praksi. Džoeel Karneval (*Joel Carnevale*) i Izabela Hatak (*Isabella Hatak*) razmatrali su problem upravljanja ljudskim resursima tokom pandemije. Oni veruju da je kriza koja je nastupila prošle godine, inicirala plodotvorna naučna istraživanja i doprinela konsolidovanju nalaza koji mogu doprineti adekvatnijoj praksi u podršci kompanijama u suočavanju sa krizama<sup>43</sup>. Autori smatraju da je potrebno istražiti na koji način se tretira odnos posao-porodica od strane zaposlenih, i koji su načini stigmatizacije pojedinih zaposlenih koji u uslovima krize "nemaju obavezu oko porodica" ukoliko su neoženjeni/neudati<sup>44</sup>. Pravovremena organizacija i planiranje međuljudskih odnosa i praćenje privatnog života u domenu organizacije vremena, za poslodavce je od velike važnosti zarad obezbeđivanja kontinuiteta poslovanja u uslovima kada kriza preči prekidom poslovnog procesa<sup>45</sup>.

Jagdiš Šet (*Jagdish Sheth*) navodi da bi korporacije trebalo da u svoje procene rizika uvrste navike potrošača na agendi svog poslovanja. Pandemija je, prema njegovim tvrdnjama, dovela do dve vrste posledica u promenama potrošačkih navika - kratkoročne, koje je moguće identifikovati već u ovoj fazi, ali i dugoročne, koje nije moguće još uvek precizirati imajući u vidu da tokom 2021. godine, pandemija još uvek traje<sup>46</sup>. U kratkoročne promene navika, ovaj autor ubraja (bespotrebno) nagomilavanje namirnica i higijenskih proizvoda, naročito sredstava za dezinfekciju i sredstava za ličnu zaštitu (maski, vizira, skafan-

<sup>42</sup> Goldstein, M., Gonzalez, P. M., Sreelakshmi P., Wimpey, J. (2020): The Global State of Small Business during COVID-19: Gender Inequalities, available at: <https://blogs.worldbank.org/developmenttalk/global-state-small-business-during-covid-19-gender-inequalities> (23.03.2021.).

<sup>43</sup> Carnevale, J., Hatak, I. (2020): Employee adjustment and well-being in the era of COVID-19: Implications for human resource management. *Journal of Business Research*, 116, 183-187 [https://www.researchgate.net/publication/341557520\\_Employee\\_Adjustment\\_and\\_Well-Being\\_in\\_the\\_Era\\_of\\_COVID-19\\_Implications\\_for\\_Human\\_Resource\\_Management](https://www.researchgate.net/publication/341557520_Employee_Adjustment_and_Well-Being_in_the_Era_of_COVID-19_Implications_for_Human_Resource_Management) (02.03.2021). str. 4.

<sup>44</sup> Ibid, str. 12.

<sup>45</sup> Ibid, str. 12.

<sup>46</sup> Sheth, J. (2020): Impact of Covid-19 on consumer behavior: Will the old habits return or die? *Journal of Business Research*, 117, 280-283.

dera i dr.), što je bila karakteristika rane faze razvoja pandemije<sup>47</sup>. Zbog toga su ovu fazu pandemije bolje prošle kompanije koje su imale efikasan sistem brzog i dinamičnog snabdevanja jer su se rafovi širom sveta praznili enormnom brzinom. Sledeća odlika promene potrošačkih navika se odnosi na improvizaciju i «pomodarstvo» u pružanju pojedinih usluga. Šet, primera radi, navodi onlajn prenose crkvenih liturgija ili venčanja, kao i koncerata<sup>48</sup>. Treća karakteristika je suprotstavljena prvoj i ogledala se u takozvanom „zadržavanju potražnje“. Naime, nasuprot kratkoročnom gomilanju namirnica i sredstava za život zbog neizvesnosti u pogledu budućih dešavanja, zadržavanje potražnje se javilo kao reakcija na njih. Takva zadržavanja se ogledaju u poništavanju avio karata, zahtevima za refundiranje novca od otkazanih događaja i slično<sup>49</sup>.

Još jedna kratkoročna promena u potrošačkim navikama ogledala se u sveopštem masovnom prihvatanju digitalne tehnologije. Šet apostrofira servise za audio i video prenos signala poput Zuma (*Zoom*), Fejsbuka (*Facebook*), Vebeksa (*Webex*), ali i društvenih medija kao što su Fejsbuk, Instagram (*Instagram*) i Jutjub (*Youtube*). Zbog toga su one kompanije koje su preusmerile svoje usluge ili poslovanje, u meri u kojoj je to bilo moguće, na ove elektronske servise, doživele porast profita tokom pandemije, bez rizika po obustavljanje proizvodnog procesa<sup>50</sup>. Naredna kratkoročna promena u odnosu na ponašanje potrošača odnosila se na «konzumerizam kod kuće». Navika da nam prodavnice budu ispred doma, brzo je osvojila simpatije čovečanstva, a kompanije koje su to uspele, nastavile su sa poslovnim uspesima<sup>51</sup>. Prethodno pobrojane promene su kao opštiju posledicu imale zamagljivanje odnosa «posao-život» jer se celokupan posao kompanijama koje svoje poslovanje mogu da realizuju radom od kuće - tako i odvijao, što je zaposlenima bilo istovremeno i prednost ali i mana<sup>52</sup>.

Iz perspektive bezbednosnog menadžmenta, pojedina istraživanja su potvrdila pretpostavku o neophodnosti planiranja i upravljanja rizicima zarad adekvatnijeg odgovora na krize, naročito one koje ostavljaju najteže posledice poput pandemije SARS - CoV 2<sup>53</sup>. Rezilijentnost koja se stvara pravovremenim identifikovanjem svih rizika u matrici rizika, potvrdila je mogućnost određenih kompanija da opstanu i u vreme najvećeg «zatvaranja» zbog epidemioloških razloga<sup>54</sup>. Takvo kvalitetno upravljanje kompanijom zasnivalo se u vreme najveće krize

---

<sup>47</sup> Ibid.

<sup>48</sup> Ibid, str. 281.

<sup>49</sup> Ibid, str. 281.

<sup>50</sup> Ibid, str. 281.

<sup>51</sup> Sheth, J. (2020): Impact of Covid-19 on consumer behavior: Will the old habits return or die? *Journal of Business Research*, 117, 280-283.

<sup>52</sup> Ibid.

<sup>53</sup> Belaj, D. (2020): Konceptualni model osiguranja kontinuiteta poslovanja temeljen na analizi rizika. Koprivnica: Sveučilište Sjever.

<sup>54</sup> Ibid.

na uspešnom upravljanju kontinuitetom poslovnog procesa. Primera radi, istraživanje koje je za studiju slučaja imalo analizu rizika i kontinuiteta poslovanja hrvatske kompanije „Podravka“ tokom 2020. godine, pokazalo je da je zbog višegodišnjeg pravovremenog planiranja i upravljanja rizicima, ova kompanija tokom krize ostvarila još veći profit nego u uobičajenim uslovima. Time je u praksi demonstriran značaj takozvanog „konceptualnog modela“ kontinuiteta poslovanja baziran na upravljanju rizicima<sup>55</sup>.

Podsetimo se na ranije izneto zapažanje da je kvalitet života zaposlenih važna karika u osiguranju kontinuiteta poslovnog procesa, u cilju ukupne produktivnosti korporacija. Arsovski i Milićević su ustanovili statistički pozitivnu korelaciju između kontinuiteta poslovanja i višeg kvaliteta života. Stoga, korporativna briga o kvalitetu života sopstvenih zaposlenih je u direktnoj vezi sa osiguranjem kontinuiteta poslovanja, što oni detaljno prikazuju kroz model integracije ove dve varijable<sup>56</sup>.

Pojedini autori, međutim, ukazuju na činjenicu da pandemija SARS - CoV 2 nije donela samo negativne posledice po svetsku privredu. Oni tretiraju ovu pretnju kao svojevrsni „filter“ koji je iznedrio mnoge kompanije, ali i grane privrede i doprineo sveopštoj globalizaciji i digitalizaciji celokupnog društva. Primera za to su svi poslovi i sve delatnosti koji su bazirani na internet tehnologijama, poput elektronske prodaje, dostave hrane, obrazovanja posredstvom onlajn alata i platformi, kao i bilo koji drugi poslovi koji se mogu efikasno obavljati putem interneta<sup>57</sup>.

Konsultantska kuća «Diloit» (*Deloitte*) objavila je krajem 2020. godine preporuke kompanijama u odgovoru na posledice pandemije izazvane virusom SARS - CoV 2. Prema izveštaju, mere treba da budu podeljene na nekoliko segmenata: na inicijalne i kratkoročne aktivnosti koje se preduzimaju poput regulisanja prevoza i putovanja zaposlenih, njihove epidemiološke zaštite i predstavljanja obezbeđivanja proizvoda svojim potrošačima kao i na ostale *post festum* mere<sup>58</sup>. Druga grupa mera obuhvata takozvane rizike po infrastrukturu poslovanja. Izveštaj daje smernice za daljinsko upravljanje sistemima i proizvodnjom, mapiranje tačaka koje su kritične u proizvodnji, regulisanje odnosa sa dobavljačima i kašnjenjem dostave repromaterijala i slično<sup>59</sup>. Sledeća grupa mera odnosi se na sajber rizike. Ona obuhvata proveru nadzora aplikacija za udaljeni pristup i njihovo testiranje, vršenje «kampanje podizanja svesti» o posebnim uslovima društvenog života zaposlenih tokom pandemije, kao i dizajniranje

<sup>55</sup> Ibid, str. 35-36.

<sup>56</sup> Арсовски, С., Милићевећ, Р. (2010): «Менаџмент континуитетом пословања и квалитет живота.» Рад презентован на Фестивалу квалитета – 5. национална конференција о квалитету живота. Крагујевац: Факултет инжењерских наука, стр. 5.

<sup>57</sup> Donthu, N., Gustafsson, A. (2020): Effects of COVID-19 on business and research. Journal of business research, 117, 284-289.

<sup>58</sup> Deloitte. (2020): COVID-19: Managing Risks and Ensuring Business Continuity, available at: <https://www2.deloitte.com/rs/en/pages/risk/articles/covid-19-managing-risk-and-ensuring-business-continuity.html> (04.04.2021.).

<sup>59</sup> Ibid.

mera za pomoć zaposlenima u slučaju poteškoća u radu sa elektronskim servisima<sup>60</sup>. Na kraju, Diloit preporučuje mapiranje tačaka koje su se pokazale neuspešnim u prvim mesecima nakon krize, zatim uspostavljanje mera i uputstava za kontinuitet poslovnog procesa, kreiranje planova reagovanja (koji uključuju postupke, raspodele zaposlenih, alate i sredstva za rad), kao i pripreme za kašnjenja u lancu snabdevanja<sup>61</sup>.

## Zaključak

Sprovedeno istraživanje je imalo za cilj da pruži uvid u najznačajnije teorijske elaboracije koje tematizuju problem kontinuiteta poslovanja korporacija tokom pandemije izazvane virusom SARS - CoV 2.

U radu su opisane i objašnjene promene u teorijskim paradigmatama korporativne bezbednosti u svetlu novih izazova kojima se ugrožava poslovni proces, iznedrenih pandemijom kao nedovoljno istraženim hazardom. Polazna pretpostavka odnosila se na neophodnost inovativnog posmatranja korporativne bezbednosti u svetlu novih netradicionalnih i asimetričnih pretnji po međunarodnu bezbednost. Funkcije korporativne bezbednosti poput sigurnosti, lične bezbednosti zaposlenih, regulisanja „vlasništva“ nad službom fizičkog obezbeđenja, obrazovanja i obuka u sferi bezbednosti, zaštita od požara i unutrašnje istrage, ostaju važne u integralnom obezbeđivanju kompanija. Sa razvojem novih tehnologija i tektonskih poremećaja koje nesvakidašnje krize poput pandemije SARS - CoV 2 donose, međutim, relativno nove funkcije poput kontinuiteta poslovanja i informacione bezbednosti dobijaju na značaju. Zbog toga je važno usmeriti pažnju kako akademske, tako i stručne, javnosti na neophodnost zaštite i održanja kontinuiteta poslovnog procesa od koga zavisi položaj i opstanak kompanije na tržištu.

Iako još uvek nisu sprovedena detaljna istraživanja o odnosu pandemije SARS - CoV 2 i kvaliteta života zaposlenih, saznanja o ovoj korelaciji će u budućnosti biti naročito značajna. Naime, radikalne promene u načinu rada i uslovima za rad, koje su izazvane pandemijom, uslovile su i promenu obrazaca ponašanja zaposlenih u velikim korporacijama. Zbog toga je važan segment održanja kontinuiteta poslovnog procesa upravo briga o zaposlenima, odnosno njihovom kvalitetu života. Ta briga ne sme biti ograničena samo na radni proces i/ili proizvodne pogone, već i na širi spektar aktivnosti koje zaposleni obavljaju mimo radnog vremena, u cilju poboljšavanja njihove produktivnosti.

Osim toga, u proces planiranja kontinuiteta poslovanja neophodno je uključiti i pretpostavku o promeni potrošačkih navika tokom pandemije. Ukoliko kompanija ne prati trendove koji se odnose na prodaju i navike potrošača ili korisnika usluga, i insistiraju na „starom“ modelu poslovanja koji se primenjivao do početka krize, teško je očekivati da će dugoročno opstati na tržištu.

<sup>60</sup> Ibid.

<sup>61</sup> Ibid.

### Literatura:

- Арсовски, С., Милићевић, Р. (2010): «Менаџмент континуитетом пословања и квалитет живота.» Рад презентован на Фестивалу квалитета – 5. национална конференција о квалитету живота. Крагујевац: Факултет инжењерских наука
- Belaj, D. (2020): *Konceptualni model osiguranja kontinuiteta poslovanja temeljen na analizi rizika*. Koprivnica: Sveučilište Sjever
- Botha, J., Von Solms, R. (2004): A cyclic approach to business continuity planning. *Information Management & Computer Security*, 12(4), 328-337
- Briggs, R., Edwards, C. (2006): *The business of Resilience: Corporate Security for the 21st Century*. London: Demos
- Carnevale, J., Hatak, I. (2020): Employee adjustment and well-being in the era of COVID-19: Implications for human resource management. *Journal of Business Research*, 116, 183-187 [https://www.researchgate.net/publication/341557520\\_Employee\\_Adjustment\\_and\\_Well-Being\\_in\\_the\\_Era\\_of\\_COVID-19\\_Implications\\_for\\_Human\\_Resource\\_Management](https://www.researchgate.net/publication/341557520_Employee_Adjustment_and_Well-Being_in_the_Era_of_COVID-19_Implications_for_Human_Resource_Management) (02.03.2021.)
- Cerullo, V., Cerullo, M. (2004): Business continuity planning: a comprehensive approach. *Information systems management*, 21, 70-78
- Deloitte. (2020): *COVID-19: Managing Risks and Ensuring Business Continuity*, available at: <https://www2.deloitte.com/rs/en/pages/risk/articles/covid-19-managing-risk-and-ensuring-business-continuity.html> (04.04.2021.)
- Donthu, N., Gustafsson, A. (2020): Effects of COVID-19 on business and research. *Journal of business research*, 117, 284-289
- Goldstein, M., Gonzalez, P. M., Sreelakshmi P., Wimpey, J. (2020): *The Global State of Small Business during COVID-19: Gender Inequalities*, available at: <https://blogs.worldbank.org/developmenttalk/global-state-small-business-during-covid-19-gender-inequalities> (23.03.2021.)
- Halibozek, E., Kovacich, G. (2017): *The manager's handbook for corporate security: establishing and managing a successful assets protection program*. Butterworth-Heinemann
- Лабус, М. (2020): *Модел адаптивног управљања континуитетом електронског пословања*. Београд: Универзитет у Београду-Факултет организационих наука
- Lippert, K., Walby, K., Steckle, R. (2013): Multiplicities of corporate security: Identifying emerging types, trends and issues. *Security Journal*, 26(3), 206-221
- Petersen, K. (2013): The corporate security professional: A hybrid agent between corporate and national security. *Security journal*, 26(3), 222-235
- Sheth, J. (2020): Impact of Covid-19 on consumer behavior: Will the old habits return or die? *Journal of Business Research*, 117, 280-283
- Williams, J. (2005): Reflections on the private versus public policing of economic crime. *The British Journal of Criminology*, 45(3), 316-339
- Wolf, K., Deitelhoff, N., Engert, S. (2007): Corporate security responsibility: Towards a conceptual framework for a comparative research agenda. *Cooperation and Conflict*, 42(3), 294-320

Goran J. Mandić  
Nenad Putnik  
Sandra Rakić

UDC 005.332:[616.98:578.834  
005.334:334.72  
005.961:005.81  
DOI: 10.5937/MegRev2104025M  
Expert article  
Received 16.06.2021.  
Approved 17.08.2021.

## BUSINESS CONTINUITY AS A FUNCTION OF CORPORATE SECURITY – SARS-CoV 2 PANDEMIC CASE STUDY

**Abstract:** *Business continuity occupies an important place both in the academic sphere and in the practical application that is carried out in order to ensure continuation of the legal entity. Multiple complex factors and threats that shape not only national but also global security, significantly affect the functioning of corporations, which makes the traditional approach to corporate security relatively outdated. The aim of this article is to present the most important discussions related to this phenomenon within the academic literature, as well as to identify issues that are important for successful theoretical development and application of this concept in business practice. The authors consider the concept of business continuity as one of the most important concepts in the function of corporate security, having in mind the challenges and threats faced by companies, especially those that orient their business towards exports to foreign markets. The pandemic caused by the SARS - CoV 2 virus, which culminated in 2020, largely showed the weaknesses of “classic” business continuity planning, bearing in mind that many companies in Serbia and around the world have completely suspended their production processes. Therefore, in this paper, on the example of a pandemic, the current weaknesses will be partially identified, as well as recommendations that would ensure the continuity of the work process and thus achieve the functionality of corporations*

**Key words:** *corporate security, corporation, business continuity, risk management, SARS - CoV 2*

