Ivana Baltezarević*
Radoslav Baltezarević**

UDK 343.533::004
004.738.5.056.53

DOI: 10.5937/MegRev2104269B
Pregledni naučni članak
Primljen 18.05.2021.
Odobren 10.09.2021.

SAJBER BEZBEDNOST: IZGRADNJA DIGITALNOG POVERENJA***

Sažetak: *Iako su informaciono-komunikacione tehnologije omogućile mnogo lakšu komunikaciju, zabavu i poslovanje ljudima, takođe su omogućile i sajber kriminalcima da vrše svoje ilegalne aktivnosti u digitalnom okruženju. Zloupotrebom podataka, ali i aktivnostima koji mogu naneti emocionalnu i fizičku štetu korisnicima interneta, sajber kriminalci doprineli su eroziji poverenja potrošača koji su svoje potrebe i želje zadovoljavali digitalnom kupovinom. U vremenima svetske pandemije, kada je veliki broj potrošača bio primoran da koristi usluge kupovine u onlajn okruženju, ovakvo nepoverenje nanelo je velike štete kompanijama. Strategije ponovne izgradnje poverenja i revitalizovanja lojalnosti potrošača, nameću se kao imperativ mnogim organizacijama, ukoliko žele da opstanu na tržištu. Naravno potrebna je i zakonodavna podrška, kako bi se obezbedila sajber bezbednost, koja sve više poprima globalne dimenzije u svom obimu, predstavljajući imperative u odbrani od sajber pretnji i samim državama, ugrožavajući njihovu ekonomsku i političku stabilnost.*

Ključne reči: *Informaciono-komunikacione tehnologije, Sajber kriminal, Digitalno poverenje, Potrošači, Sajber bezbednost*

* Docent, Pravni fakultet, Megatrend Univerzitet, Beograd; ivana.baltezarevic@gmail.com

** Redovni professor, Fakultet za poslovne studije, Megatrend Univerzitet, Beograd; rbaltezarevic@gmail.com

*** Ovaj rad je rezultat projekta Pravnog fakulteta FPPNT –Pravo i nove tehnologije i projekta Fakulteta za poslovne studije : FPSBPS Budućnost poslovanja u Srbiji

1. Uvod

Tradicionalni oblik komunikacije na Internetu drastično se promenio. Savremene tehnologije značajno su doprinele redefinisanju komunikacije uz podršku IT mreže, što povećava i rizik i uslovljavanje sistema vrednosti. Može se reći da novo doba zahteva nove komunikacijske veštine.[1] Internet i društvene mreže utiču na mnoge aspekte života ljudi u savremenom okruženju i imaju dubok uticaj u međuljudskoj komunikaciji. Vremenom će nastaviti da se sve više integrišu u ljudsko iskustvo i da povećavaju obim komunikacijskog procesa.[2]

Pretnje nasiljem u digitalnom okruženju mogu uključivati uznemiravanje od strane dva ili više lica protiv pojedinca ili više osoba (Zakon o zaštiti od uznemiravanja iz 1997. godine). Ne postoji zakonska definicija sajber uhođenja, niti postoje posebni zakoni koji bi se pozabavili takvim ponašanjem. Generalno, sajber uhođenje se opisuje kao preteće ponašanje ili neželjena aktivnost usmerena na drugog, korišćenjem oblika onlajn komunikacije. Sajber uhođenje i onlajn uznemiravanje često se kombinuju sa drugim oblicima „tradicionalnog" uhođenja ili uznemiravanja, poput praćenja ili primanja neželjenih telefonskih poziva ili pisama. Primeri uvredljivog ponašanja mogu uključivati: preteće ili opscene e-poruke ili tekstualne poruke; uznemiravanje uživo ili ponižavanje vršnjaka na mreži, označavajući ih seksualno promiskuitetnim; ostavljanje neprikladnih poruka na mrežnim forumima ili oglasnim tablama; neželjeni indirektni kontakt sa osobom koji može biti preteći, kao što je objavljivanje slika dece ili radnog mesta te osobe na veb lokaciji društvenih medija, bez ikakvog pozivanja na ime ili nalog osobe; postavljanje „fotošopiranih" slika osoba na platformama društvenih medija; slanje neželjenih e-poruka; spamovanje, gde prestupnik šalje žrtvi više neželjenih e-poruka; hakovanje naloga društvenih medija, a zatim praćenje i kontrola naloga; distribucija zlonamernog softvera; krađa sajber identiteta itd.[3]

Pitanje koje sve češće postavljaju korisnici internet tehnologija i društvenih mreža je koji se izvori informacija mogu smatrati kredibilnim, odnosno na koji način se mogu identifikovati digitalni izvori u koje korisnici prilikom interakcije

[1] Baltezarević Radoslav & Baltezarević Vesna (2016): Virtual communication's skills - view through the social media and situation in Serbia. In M. Radovic-Markovic, I. S. Kyaruzi & Z. Nikitovic (Eds.). *Entrepreneurship: types, current trends and future perspectives* (pp. 275-287). Graphics, Inc. Chicago, United States of America; Akamai University, Hilo, United States of America; Faculty of Business Economics and Entrepreneurship (BEE), Belgrade, Serbia; Institute of Social Entrepreneurship (IRESEED), Great Britain ISBN: 978-1-5323-2194-8.

[2] Baltezarević Ivana & Baltezarević Radoslav (2020): Uticaj komunikacije u virtuelnom okruženju na pravnu informatiku, *Megatrend revija* Vol. 17, № 4, 2020: 27-40. DOI: 10.5937/MegRev2004027B.

[3] CPS (Crown Prosecution Service). (n.d.): *Guidelines on prosecuting cases involving communications sent via social media* https://www.cps.gov.uk/legal-guidance/social-media-guidelines-prosecuting-cases-involving-communications-sent-social-media (Pristupljeno: 05.10.2021.)

mogu imati poverenja u smislu da im neće biti naneta bilo kakva emocionalna ili materijalna šteta usled nezakonitih sajber aktivnosti.

MekAlister (McAllister) objašnjava poverenje kao meru u kojoj je osoba uverena i spremna da deluje na osnovu reči, postupaka i odluka drugog[4] i empirijski identifikuje poverenje zasnovano na kognitivnim i efektima kao zasebni konstrukt. Ova kombinacija pogleda i nalaza pruža nam definiciju poverenja među pojedincima (tj. međuljudsko poverenje). Međutim, poverenje se javlja i na nivou organizacije (organizaciono poverenje) i empirijski je utvrđeno da se razlikuje od međuljudskog poverenja.[5] Kuelh i Klejn (Quelch i Klein) spekulišu da je poverenje u ranim fazama razvoja interneta kritičan faktor u podsticanju kupovine preko interneta.[6] Kin (Keen) upozorava da poverenje nije samo kratkoročno pitanje, već i najznačajnija dugoročna barijera za ostvarivanje potencijala internet marketinga za potrošače.[7]

Elektronska trgovina, koja je eskalirala u doba pandemije suočava se sa niskim poverenjem potrošača, naravno usled mnogobrojnih zloupotreba podataka korisnika, prevara i drugih kriminalnih sajber aktivnosti. Iz tog razloga kompanije moraju razviti nove strategije u cilju povećanja nivoa poverenja na relaciji potrošač – kompanija.

2. Sajber maltretiranje, sajber uznemiravanje i sajber uhođenje

Sajber maltretiranje, sajber uznemiravanje i sajber uhođenje su termini koji pokrivaju različite oblike ponašanja koji pokazuju slične karakteristike. Ponekad se termini koriste naizmenično, a ponekad se razlikuju. Maltretiranje i uznemiravanje mogli bi se smatrati različitim od uhođenja, iako među njima postoji određeno preklapanje. Zlostavljanje i uznemiravanje uključuju individualizirano negativno ponašanje, pri čemu se neko ponaša agresivno ili neprijateljski kako bi zastrašio žrtvu. Ovo uključuje različite vrste ponašanja, kao što su: raspirivanje (objavljivanje provokativnih ili uvredljivih postova), objavljivanje ili zloupotrebu ličnih podataka i/ili distribuciju zlonamernog softvera. Sajber uhođenje može uključivati: komunikaciju sa žrtvom (i pasivne i agresivne oblike), objavljivanje informacija o žrtvi, ciljanje računara žrtve (posebno radi dobijanja ličnih podataka), stavljanje žrtve pod nadzor, uključujući sajber-nadzor). Osim krajnjeg faktora, postoje sličnosti između sajber uhođenja i sajber maltretiranja u

[4] McAllister, D.J. (1995): 'Affect- and cognition- based trust as foundations for interpersonal cooperation in organizations', *Academy of Management Journal*, 38: 24–59.

[5] Doney, P.M. & J.P. Cannon (1997): 'An examination of the nature of trust in buyer– seller relationships', *Journal of Marketing*, 61: 35–51.

[6] Quelch, J.A. & L.R. Klein (1996): 'The Internet and international marketing', *Sloan Management Review*, 37(3): 60–75.

[7] Keen, P.G.W. (1997): 'Are you ready for "trust" economy?', *Computer World*.

smislu načina na koji su krivična dela počinjena.[8] U današnje vreme postoji širok spektar krivičnih dela u gore navedenim kategorijama koji se koriste za krivično gonjenje zlostavljanja sprovedenog na mreži, npr. putem društvenih mreža. Jedna takva kategorija uključuje komunikacije koje mogu predstavljati pretnju nasiljem po osobu.[9] Ako mrežna komunikacija uključuje pretnju ubistvom, može se pokrenuti krivični postupak prema s16 Zakona o prekršajima protiv lica iz 1861. godine. Druge pretnje nasiljem po osobu mogu se uzeti u obzir prema odredbama Zakona o zaštiti od uznemiravanja iz 1997. godine, naime, odjeljak 4 (stavljanje drugog u strah od nasilja) ili 4A (uhođenje koje uključuje strah od nasilja ili ozbiljnu uzbunu ili uznemirenost), ako predstavljaju način ponašanja koji predstavlja uznemiravanje ili uhođenje. Pretnje nasiljem nad osobom ili oštećenje imovine takođe se mogu uzeti u obzir prema članu 1 Zakona o zlonamernim komunikacijama iz 1988. godine, koji zabranjuje slanje elektronske komunikacije koja predstavlja pretnju, ili članu 127 Zakona o komunikacijama iz 2003. godine koji zabranjuje slanje poruka „pretećeg karaktera" putem javne telekomunikacione mreže. Uvredljive komunikacije poslane putem društvenih medija koje ciljaju određenu osobu ili pojedince mogu se uzeti u obzir pod odeljcima 2, 2A, 4 ili 4A Zakona o zaštiti od uznemiravanja iz 1997. godine, ako predstavljaju krivično delo uznemiravanja ili uhođenja, ili članu 76 Zakona o teškom zločinu iz 2015. godine, ako predstavljaju krivično delo kontrole ili prinudnog ponašanja. Uznemiravanje može uključivati ponovljene pokušaje nametanja neželjene komunikacije ili kontakta pojedincu na način za koji se može očekivati da će izazvati uznemirenost ili strah kod bilo koje razumne osobe.[10]

Da li bilo koja od ovih sajber aktivnosti predstavlja prekršaj zavisiće od konteksta i posebnih okolnosti dotične radnje. Zakon o zaštiti od uznemiravanja iz 1997. godine zahteva od tužilaštva da dokaže da je okrivljeni sledio način ponašanja koji se odnosio na uznemiravanje ili uhođenje. Zakon navodi da „način ponašanja" mora uključivati ponašanje u najmanje dva navrata. Dotično ponašanje mora činiti niz događaja. Svaki pojedinačni čin koji čini deo ponašanja ne mora imati dovoljnu težinu da sam po sebi predstavlja zločin; međutim, što je manje incidenata, svaki će verovatno morati da bude ozbiljniji da bi tok ponašanja bio uznemiravanje. Tamo gde pojedinac prima neželjenu komunikaciju od druge osobe putem društvenih medija, pored drugog neželjenog ponašanja van mreže, sve to treba zajedno razmotriti kako bi se utvrdilo da li je reč o ilegalnom načinu ponašanja ili ne. Komunikacija poslata putem društvenih medija može sama ili zajedno sa drugim ponašanjem predstavljati prekršaj kontrole ili prisilnog pona-

[8] Gillespie, A. (2016): *Cybercrime: Key issues and debate*. Oxford: Routledge ISBN 978-0-415-71220-0.

[9] CPS (Crown Prosecution Service). (n.d.). *Guidelines on prosecuting cases involving communications sent via social media* https://www.cps.gov.uk/legal-guidance/social-media-guidelines-prosecuting-cases-involving-communications-sent-social-media (Pristupljeno: 05.10.2021.)

[10] Ibid

šanja u intimnoj ili porodičnoj vezi prema članu 76 Zakona o teškom zločinu iz 2015. godine. Ovaj prekršaj odnosi se samo na počinioce i žrtve koji su lično povezani: u intimnoj ličnoj vezi; žive zajedno i prethodno su bili u intimnoj ličnoj vezi; ili žive zajedno i članovi su porodice. Dotično kontrolirajuće ili prisilno ponašanje mora se ponavljati kontinuirano i mora imati ozbiljan učinak na žrtvu, a počinitelj mora znati ili bi trebao znati da će ponašanje imati takav učinak.[11]

3. Sigurnost i poverenje u sajber prostor

Nema sumnje da tehnologija koju koristi veliki broj kompanija, uključujući finansijske institucije, primetno u zemljama u razvoju, postaje sve raznovrsnija, naprednija i inovativnija. Prilikom merenja jaza između finansijskih institucija koje su tehnološki orijentisane i onih koji to nisu, nalazi se značajna razlika. Međunarodna unija za telekomunikacije identifikovala je pet ključnih faktora za uspeh programa sajber bezbednosti na nacionalnom nivou; to su: (a) nacionalna strategija; (b) saradnja između vlade i industrije; (v) čvrsta pravna osnova za odvraćanje od sajber kriminala; (g) nacionalna sposobnost upravljanja incidentima; i (d) nacionalna svest o važnosti sajber bezbednosti.[12] Napadi i neovlašćeno korišćenje kompanija i institucija uključuju zlonamerne radnje kao što su krađa ili uništavanje intelektualne svojine, zloupotreba od strane insajdera i neovlašćeni pristup informacijama koji za posledicu imaju gubitak integriteta i poverljivosti podataka, kao i pretnje zlonamernim softverom, poput virusa, špijunskih softvera, crva (worms) i trojancima. Ovi sajber napadi utiču na poverenje sajber korisnika i kao takvi dovode do bojazni o korišćenju interneta kao sredstva za obavljanje transakcija, ali i za samu komunikaciju u digitalnom okruženju. Filozofi, kada raspravljaju o „poverenju", često se pozivaju na jednu stranu koja pokazuje poverenje u drugu, ali se oseća ranjivom na ponašanje druge strane. Drugim rečima, ako verujete nekome, prihvatate da, iako je to teoretska mogućnost, nije realna verovatnoća da će se ponašati na način koji bi vas ugrozio. Koncepti poverenja i bezbednosti privukli su veliku pažnju u novijoj literaturi u ovoj oblasti. Raspravljalo se o tome šta je poverenje; šta znači njegov uticaj na aktivnosti na mreži, koji je njegov doprinos u širenju aktivnosti u sajber prostoru itd. Veliki deo ove literature je iz polja organizacionog ponašanja. Ono što je još važnije, takođe se sve više koristi koncept poverenja u kompanije zasnovane na internetu. Izraz „poverenje" koriste ljudi koji se bave bezbednošću informacija i sajber prostorom. Najpopularniji domen za njegovu upotrebu bilo je istraživanje autentifikacije i infrastrukture za tehnologiju javnih ključeva (public keys) u umreženom

[11] Ibid

[12] Ennis, J. (2008): 'Best practices for organizing national cyber security efforts', presentation made at regional workshop organized by the ITU in collaboration with *ictQATAR* and *Q-CERT*, 18-21 February

okruženju. Pitanje načina razmene javnih ključeva i njihovih sertifikata putem interneta bilo je važno za tvorce i korisnike aplikacija za javne ključeve. Međutim, šira, tradicionalnija upotreba reči - izvan specifikacija formata sertifikata za javne ključeve - povećala se sa porastom sajber aktivnosti. Iako se često koristi izraz „poverenje", ono se retko definiše. Poverenje je delimično definisano Vebsterovim rečnikom kao čvrsto oslanjanje na integritet, sposobnost ili karakter osobe ili stvari ili oslanjanje na nameru i sposobnost kupca da plati u budućnosti. Obe ove definicije govore o zdravom razumevanju poverenja. Ako vam verujem, oslanjam se na kvalitet ili atribut nečega, ili na istinitost izjave. Takođe nagoveštava logičan tretman koji bi se mogao primeniti na razumevanje poverenja u odnos. Poverenje je stanje koje uključuje poverljiva pozitivna očekivanja o tuđim motivima u odnosu na vlastito ja u situacijama koje uključuju rizik[13] i stoga je orijentacija prema drugima koja je izvan racionalnosti,[14] jer povećava nečiju ranjivost na oportunističko ponašanje.[15] Zahir i sar. (Zaheer) opisuju organizaciono poverenje kao stepen u kojem članovi organizacije imaju kolektivnu orijentaciju poverenja prema partnerskoj kompaniji.[16] Ova definicija se u velikoj meri poklapa sa razumevanjem poverenja na makro nivou u sociologiji. Na primer, Kolman (Coleman) pojašnjava poverenje na makro nivou kao generalizaciju sistema uzajamnog poverenja sa dva aktera, ali uključuje i veći broj aktera. Kolman takođe tvrdi da postoji neka vrsta povratne informacije između makro i mikro nivoa.[17]

Menadžersko istraživanje o organizacijskom poverenju uglavnom se slaže da je ono dobro za performanse, ali rezultati istraživanja o međuljudskom poverenju su manje jasni. Na primer, istraživanje Čoua i Holdena (Chow i Holden) nudi snažnu podršku značaju međuljudskog poverenja,[18] dok su Zahir i kolege otkrili da je njegova funkcija manje važna od poverenja u organizaciju.[19] Jasno je da je potrebna teorija većeg obima pre nego što se značaj i efekti poverenja potpunije spoznaju i istaknu. Postojeći empirijski dokazi, međutim, podržavaju

[13] Boon, S.D. & J.G. Holmes (1991): 'The dynamics of interpersonal trust: resolving uncertainty in the face of risk', in R.A. Hinde & J. Grobel (eds), *Cooperation and Prosocial Behavior, Cambridge: Cambridge University Press*, pp. 190–211

[14] Tyler, Tom R. & Roderick M. Kramer (1996): 'Whither trust?', in *Trust in Organizations, Frontiers of Theory and Research*, in Roderick M. Kramer and Tom Tyler, Thousand Oaks, CA: Sage.

[15] Cummings, L.L. & P. Bromiley (1996): 'The organizational trust inventory', in R. Kramer and T. Tyler (eds), *Trust in Organizations*, Thousand Oaks, CA: Sage, pp. 302–30

[16] Zaheer, A., B. McEvily & V. Perrone (1998): 'Does trust matter? Exploring the effects of interorganizational and interpersonal trust on performance', *Organization Science*, 9: 141–59.

[17] Coleman, J.S. (1990): *Foundations of Social Theory*, Cambridge, MA: Belknap Press of Harvard University Press.

[18] Chow, S. & R. Holden (1997): 'Toward an understanding of loyalty: the moderating role of trust', *Journal of Managerial Issues*, 9: 275–98.

[19] Zaheer, A., B. McEvily & V. Perrone (1998): 'Does trust matter? Exploring the effects of interorganizational and interpersonal trust on performance', *Organization Science*, 9: 141–59.

MekAlisterovo otkriće da poverenje ima i kognitivne i dimenzije zasnovane na afektu.[20] Poverenje zasnovano na kognitivnoj sposobnosti odražava tehničku kompetenciju i neophodnu obavezu izvršenja[21] i zasnovano je na predvidljivosti, ponašanju iz prošlosti, pouzdanosti i pravičnosti.[22] Oslanja se na racionalnu procenu sposobnosti drugog da izvršava obaveze. Za razliku od poverenja zasnovanog na kognitivnosti, poverenje zasnovano na afektu ukorenjeno je u emocionalnoj vezanosti i promišljenosti i brizi za dobrobit druge strane.[23] Postoji sama vrednost odnosa i uverenje da se druga strana oseća isto.[24]

Eksperimentalno ispitivanje internetskih korisnika sa sedištem u SAD-u, za kupovinu putem interneta, otkrilo je da su potrošači fascinirani mogućnostima međunarodne kupovine na internetu, ali su skeptični u pogledu kupovine na stranim veb stranicama.[25] Druge studije pokazuju široko rasprostranjeno nepoverenje potrošača prema trgovcima na internetu. Shodno tome, uloga poverenja izaziva velike neizvesnosti u vezi sa prodajom na internetu. Malo je verovatno da će potrošači podržati elektronske prodavnice koje ne uspevaju da stvore osećaj poverenja. Poverenje može postojati samo ako potrošač veruje da prodavac ima i sposobnost i motivaciju da isporuči robu i usluge kvaliteta očekivanog od potrošača. Ovo poverenje uglavnom je teže stvoriti za poslovanje zasnovanom na internetu nego u tradicionalnom poslovanju. U sajber prostoru, provajderi zavise od bezlične elektronske prodavnice koja će delovati u njihovo ime. Osim toga, internet smanjuje resurse potrebne za ulazak i izlazak sa tržišta. Takođe, internetske kompanije bi se mogle smatrati kao one koje su na raspolaganju potrošačima „non-stop". U tradicionalnom kontekstu, pokazalo se da je poverenje potrošača ugroženo ulaganjem prodavca u fizičke zgrade, objekte i osoblje. Elektronske prodavnice se stoga suočavaju sa situacijom u kojoj se može očekivati da je poverenje potrošača inherentno nisko, pa se kao takve moraju razviti i usvojiti određene strategije za povećanje nivoa poverenja u kompanije zasnovane na internetu.[26]

[20] Johnson, J.L., T. Sakano, K. Voss, H. Takenouchi (1998): 'Marketing performance in U.S.–Japanese cooperative alliances: eff ects of multiple dimensions of trust and commitment in the cultural interface', published in Washington State University, working paper, *Journal of the Academy of Marketing Science*, 23(4):255–71.

[21] Butler, J.K. (1983): 'Reciprocity of trust between professionals and their secretaries', *Psychological Reports*, 53: 411–16.

[22] Rempel, J.K., J.G. Holmes & M.P. Zanna (1985): 'Trust in close relationships', *Journal of Personality and Social Psychology*, 49: 95–112.

[23] Lewis, D.J. & Andrew Weigert (1985): 'Trust as social reality', *Social Forces*, 63(4) (June): 967–85.

[24] Rempel, J.K., J.G. Holmes & M.P. Zanna (1985): 'Trust in close relationships', *Journal of Personality and Social Psychology*, 49: 95–112.

[25] Jarvenpaa, S.L. & P.A. Todd (1997): 'Consumer reactions to electronic shopping on the World Wide Web', *Journal of Electronic Commerce*, 1(2): 59–88.

[26] Doney, P.M. & J.P. Cannon (1997): 'An examination of the nature of trust in buyer– seller relationships', *Journal of Marketing*, 61: 35–51.

4. Zaključak

Digitalne tehnologije postale su sastavni deo modernog društva. Olakšavaju poslovanje, komunikaciju i generalno utiču na kvalitet svakodnevnog života. Međutim, druga strana priče je da je sajber prostor takođe pogodno okruženje za različite vrste kriminalnih aktivnosti. Sajber kriminalci mogu naneti veliku materijalnu i emocionalnu štetu digitalnim korisnicima. Ove aktivnosti postaju veliki problem sa kojima se suočavaju obični ljudi, sistemi malih i velikih preduzeća, ali i same države. O ovom pitanju se široko raspravlja na međunarodnom nivou, ali čini se da sajber kriminalci uvek pronalaze nova kreativna rješenja za zaobilaženje svih sigurnosnih mera kako bi izvršili svoje kriminalne aktivnosti. Utisak je da je potrebno mnogo više odlučnosti i posvećenosti, kao i adekvatne edukacije korisnika digitalnih tehnologija kako bi prepoznali i sprečili ove pretnje iz digitalnog okruženja.[27]

Veliki broj primera iz prakse, koji svedoče o aktivnostima sajber kriminalaca i velikim posledicama koje ovakve aktivnosti nanose državama, kompanijama i pojedincima izazvale su pojavu nepoverenja i u trgovinu koja se odvija u digitalnom okruženju. Naravno takva percepcija potrošača, utiče negativno na imidž kompanija koje su usmerene na poslovanje u virtuelnom okruženju što direktno utiče na profit, a samim tim i na opstanak ovakvih organizacija na tržištu. Obzirom da je situacija izazvana globalnom pandemijom uslovila potrošače da većinu kupovine obavlja digitalnim putem, sve je veći imperativ da kompanije izgrade nove strategije koje će regenerisati poljuljano poverenje potrošača. Takođe, na nivou država, neophodno je doneti jasnije zakone i adekvatno identifikovati i sankcionisati počinitelje nezakonitih sajber aktivnosti.

[27] Baltezarević Radoslav & Baltezarević Ivana (2021): "The Dangers and Threats that Digital Users Face in Cyberspace". *IPSI Transactions on Internet Research*, Vol. 17, No. 1, January 2021, pp. 46-52.

Literatura:

- Baltezarević Radoslav & Baltezarević Vesna (2016): Virtual communication's skills - view through the social media and situation in Serbia. In M. Radovic-Markovic, I. S. Kyaruzi & Z. Nikitovic (Eds.). *Entrepreneurship: types, current trends and future perspectives* (pp. 275-287). Graphics, Inc. Chicago, United States of America; Akamai University, Hilo, United States of America; Faculty of Business Economics and Entrepreneurship (BEE), Belgrade, Serbia; Institute of Social Entrepreneurship (IRESEED), Great Britain ISBN: 978-1-5323-2194-8.
- Baltezarević Radoslav & Baltezarević Ivana (2021): "The Dangers and Threats that Digital Users Face in Cyberspace". *IPSI Transactions on Internet Research*, Vol. 17, No. 1, January 2021, pp. 46-52.
- Baltezarević Ivana & Baltezarević Radoslav (2020): Uticaj komunikacije u virtuelnom okruženju na pravnu informatiku, *Megatrend revija* Vol. 17, № 4, 2020: 27-40. DOI: 10.5937/MegRev2004027B.
- Boon, S.D. & J.G. Holmes (1991): 'The dynamics of interpersonal trust: resolving uncertainty in the face of risk', in R.A. Hinde and J. Grobel (eds), *Cooperation and Prosocial Behavior*, *Cambridge: Cambridge University Press*, pp. 190–211
- Butler, J.K. (1983): 'Reciprocity of trust between professionals and their secretaries', *Psychological Reports*, 53: 411–16.
- Chow, S. and R. Holden (1997): 'Toward an understanding of loyalty: the moderating role of trust', *Journal of Managerial Issues*, 9: 275–98.
- Coleman, J.S. (1990): *Foundations of Social Theory*, Cambridge, MA: Belknap Press of Harvard University Press.
- CPS (Crown Prosecution Service). (n.d.-a): *Guidelines on prosecuting cases involving communications sent via social media* https://www.cps.gov.uk/legal-guidance/social-media-guidelines-prosecuting-cases-involving-communications-sent-social-media (Pristupljeno: 05.10. 2021.)
- Cummings, L.L. & P. Bromiley (1996): 'The organizational trust inventory', in R. Kramer and T. Tyler (eds), *Trust in Organizations*, Thousand Oaks, CA: Sage, pp. 302–30
- Doney, P.M. and J.P. Cannon (1997): 'An examination of the nature of trust in buyer– seller relationships', *Journal of Marketing*, 61: 35–51.
- Ennis, J. (2008): 'Best practices for organizing national cyber security efforts', presentation made at regional workshop organized by the ITU in collaboration with *ictQATAR* and *Q- CERT*, 18-21 February
- Gillespie, A. (2016): *Cybercrime: Key issues and debate*. Oxford: Routledge ISBN 978-0-415-71220-0.
- Jarvenpaa, S.L. & P.A. Todd (1997): 'Consumer reactions to electronic shopping on the World Wide Web', *Journal of Electronic Commerce*, 1(2): 59–88.

- Johnson, J.L., T. Sakano, K. Voss, H. Takenouchi (1998): 'Marketing performance in U.S.–Japanese cooperative alliances: eff ects of multiple dimensions of trust and commitment in the cultural interface', published in Washington State University, working paper, *Journal of the Academy of Marketing Science*, 23(4):255–71.
- Keen, P.G.W. (1997): 'Are you ready for "trust" economy?', *Computer World*.
- Lewis, D.J. & Andrew Weigert (1985), 'Trust as social reality', *Social Forces*, 63(4) (June): 967–85.
- McAllister, D.J. (1995): 'Affect- and cognition- based trust as foundations for interpersonal cooperation in organizations', *Academy of Management Journal*, 38: 24–59.
- Quelch, J.A. and L.R. Klein (1996): 'The Internet and international marketing', *Sloan Management Review*, 37(3): 60–75.
- Rempel, J.K., J.G. Holmes and M.P. Zanna (1985): 'Trust in close relationships', *Journal of Personality and Social Psychology*, 49: 95–112.
- Tyler, Tom R. and Roderick M. Kramer (1996): 'Whither trust?', in *Trust in Organizations, Frontiers of Theory and Research*, in Roderick M. Kramer and Tom Tyler, Thousand Oaks, CA: Sage.
- Zaheer, A., B. McEvily & V. Perrone (1998): 'Does trust matter? Exploring the effects of interorganizational and interpersonal trust on performance', *Organization Science*, 9: 141–59.

Ivana Baltezarević
Radoslav Baltezarević

UDC 343.533::004
004.738.5.056.53

DOI: 10.5937/MegRev2104269B
Review scientific article
Received 18.05.2021.
Approved 10.09.2021.

CYBER SECURITY: BUILDING DIGITAL TRUST

Abstract: *Although information and communication technologies have made communication, entertainment and business easier for people, they have also enabled cybercriminals to carry out their illegal activities in the digital environment. By misusing data, but also by activities that can cause emotional and physical damage to Internet users, cybercriminals have contributed to the erosion of the trust of consumers who have satisfied their needs and desires with digital shopping. In times of global pandemic, when a large number of consumers were forced to use online shopping services, this distrust caused great damage to companies. Strategies to rebuild trust and revitalize consumer loyalty are imperative for many organizations if they want to survive in the marketplace. Of course, legislative support is also needed to ensure cyber security, which is increasingly taking on global dimensions in its scope, presenting imperatives in defense against cyber threats to states themselves, threatening their economic and political stability.*
Keywords: *Information and communication technologies, Cyber criminal, Digital trust, Consumers, Cyber security*