Lidija M. Zečević*

Pregledni naučni rad
UDK 342.738:005.334:004.056
doi: https://doi.org/10.56461/rep270125.05.Z

ZAŠTITA PODATAKA O LIČNOSTI U OKVIRIMA KORPORATIVNOG UPRAVLJANJA

Sažetak

Članak analizira odnos korporativnog upravljanja, sajber bezbednosti i zaštite podataka o ličnosti. Autor upućuje na domaće izvore i relevantne pravne norme, ističući činjenicu da srpsko pravo još uvek nije prepoznalo neophodnost detaljnog regulisanja ove materije. Stoga, članak ima za cilj da istakne trendove u stranoj literaturi i praksi na koje bi srpsko pravo moglo da se ugleda.

U prvom delu rada autor ukazuje na značaj podataka o ličnosti i važnost njihove pravne zaštite. U drugom delu rada autor analizira sajber bezbednost kao novi rizik poslovanja i daje objašnjenje na koji način korporativno upravljanje može da odgovori izazovima. U trećem delu rada autor analizira različite slučajeve sajber napada koji su doveli do kompromitacije podataka o ličnosti u najvećim kompanijama na tržištu, kao i značajne finansijske posledice koji su takvi sajber napadi imali na poslovanje kompanija.

Autor dalje zaključuje da kompromitacija podataka može biti vrlo iscrpljujuća za kompanije i još jednom podvlači potrebu za ispitivanjem (ne)adekvatnosti i (ne) spremnosti postojeće pravne regulative da odgovori novim izazovima savremenog poslovanja.

Ključne reči: korporativno upravljanje, kompromitacija podataka, zaštita podataka o ličnosti, sajber bezbednost, Opšta uredba o zaštiti podataka (GDPR).

I Uvod

Pravna zaštita podataka o ličnosti je potreba novijeg datuma i vezuje se za kraj 20. veka, a kao „preteča"[1] prava na zaštitu podataka o ličnosti uzima se

* Autor je studentkinja treće godine doktorskih studija na Pravnom fakultetu Univerziteta u Beogradu, e-mail: lidijapzecevic@gmail.com, ORCID: https://orcid.org/0009-0003-0643-0802
Rad je primljen 10. juna 2025. godine, a prihvaćen za objavljivanje 20. juna 2025. godine.

[1] S. Andonović, D. Prlja, *Osnovi prava zaštite podataka o ličnosti*, Institut za uporedno pravo, Beograd 2020, 39.

pravo na privatnost, ustanovljeno 1890. godine[2]. Pravo na privatnost je zaštićeno najvažnijim međunarodnim konvencijama kao osnovno ljudsko pravo[3] i stoga se može zaključiti da je zaštita podataka o ličnosti od izuzetnog značaja, i kao takva, zavređuje posebnu pažnju i adekvatno regulisanje u svim segmentima jednog pravnog sistema.

Potreba za balansiranjem između inovacija i zaštite privatnosti dolazi do izražaja sa pojavom digitalnih tehnologija, društvenih mreža i veštačke inteligencije, koje umnogome olakšavaju komunikaciju i poslovanje. Pored toga, kompanije se sve više okreću digitalnom poslovanju, nedovoljno spremne za sve rizike koje takvo poslovanje sa sobom nosi. Sa druge strane, korisnici uglavnom nisu dovoljno informisani i ne čitaju tzv. „politike privatnosti" kompanija, već samo popunjavaju tražene podatke o ličnosti, nesvesni načina na koji se ti podaci koriste i pohranjuju, kao i mogućih zloupotreba u različite svrhe i ozbiljnih posledica koje zloupotrebe sa sobom nose.

Cilj ovog rada jeste da ukaže na značaj dobre prakse korporativnog upravljanja za adekvatnu zaštitu podataka o ličnosti, a samim tim i prava na privatnost. Sajber bezbednosni rizici predstavljaju nove rizike poslovanja, a budući da je zadatak korporativnog upravljanja upravo upravljanje rizicima, neophodno je detaljno analizirati pravne aspekte i mehanizme zaštite podataka o ličnosti u okviru kompanije.

Neki autori zagovaraju postojanje distinkcije između poverljivosti podataka i zaštite podataka o ličnosti, a ona se zasniva na pretpostavci da poverljivost podataka štiti informacije u posedu kompanije od neovlašćenog pristupa, dok zaštita podataka o ličnosti štiti pravo na privatnost i druga prava individue[4]. Autor stoji na stanovištu da je poverljivost podataka u posedu kompanije integralni deo zaštite podataka o ličnosti, te za potrebe ovog rada sveobuhvatno analizira slučajeve neovlašćenog (ponegde i malicioznog) pristupa podacima o korisnicima određenih kompanija, i ispituje (ne)adekvatnost odgovora kompanija na takve incidente. Na mestima gde je oportuno, autor upućuje na relevantne domaće izvore i pozitivnopravne norme, ali je važno napomenuti

---

[2] *Ibid.*, 38.

[3] Vidi član 12 Univerzalne deklaracije Ujedinjenih nacija o ljudskim pravima; član 8 Evropske konvencije za zaštitu ljudskih prava i osnovnih sloboda.

[4] Ministry of Internal Affairs and Communications, Ministry of Economy, Trade and Industry of Japan, The Guidebook for Corporate Privacy Governance in the Digital Transformation (DX) Era, Ver 1.3, 2023, 20, https://www.meti.go.jp/policy/it_policy/privacy/guidebook_ver1.3_english.pdf, posećeno: 21. 3. 2025.

da srpskoj pravnoj misli nedostaju naučni radovi na ovu temu, a privrednim subjektima nedostaje svest o značaju regulisanja ove materije.

II Podaci o ličnosti i njihov značaj

Podaci o ličnosti predstavljaju „jedan od najvažnijih resursa savremene privrede i neophodan element komunikacije"[5]. Posmatrajući širu sliku, neadekvatna zaštita podataka o ličnosti podriva i inovacije[6].

Evropska unija je prepoznala neophodnost regulisanja ove materije i 2016. godine donela je Opštu uredbu o zaštiti podataka EU[7] (u daljem tekstu: GDPR). Zapravo, ističe se da GDPR „predstavlja odgovor na potrebu da lični podaci budu pažljivo prikupljani, obrađivani i čuvani"[8]. Predviđene su izuzetno stroge i visoke novčane kazne za povrede podataka o ličnosti, dok, sa druge strane, visoke novčane kazne se mogu smatrati najboljim načinom „za prevenciju od budućih zloupotreba podataka o ličnosti"[9].

Pored nadnacionalne regulative, važno je objasniti i pozitivnopravnu regulativu u Srbiji. Zaštita podataka o ličnosti je podignuta na viši nivo, budući da je garantovana članom 42 Ustava Republike Srbije, u okviru ljudskih i manjinskih prava i sloboda[10], a 2018. godine donet je Zakon o zaštiti podataka o ličnosti (dalje: ZZPL)[11].

Zakon o zaštiti podataka o ličnosti, u skladu sa definicijom GDPR[12], definiše podatak o ličnosti kao „svaki podatak koji se odnosi na fizičko lice čiji je

---

[5] S. Andonović, D. Prlja, *op. cit*., 33.

[6] Ministry of Internal Affairs and Communications, Ministry of Economy, Trade and Industry of Japan, *op. cit*., 13.

[7] Opšta uredba o zaštiti podataka EU - Regulation 2016/679 of the European Parliament and of the Council on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), od 27. 04 2016

[8] S. Prlja, Pravo na zaštitu ličnih podataka u EU, *Strani pravni život* 62(2018)1, 97.

[9] D. Prlja, G. Gasmi, „Evropska praksa zaštite pojedinaca od zloupotrebe podataka o ličnosti", u: *Zaštita podataka o ličnosti u Srbiji: zbornik radova* (ur. S. Andonović, D. Prlja, A. Diligenski), Institut za uporedno pravo, Beograd 2020, 135

[10] Ustav Republike Srbije, *Sl. glasnik RS*, br. 98/2006 i 115/2021.

[11] Zakon o zaštiti podataka o ličnosti, *Sl. glasnik RS*, br. 87/2018.

[12] Član 4(1) Opšte uredbe o zaštiti podataka EU (GDPR).

identitet određen ili odrediv, neposredno ili posredno, posebno na osnovu oznake identiteta, kao što je ime i identifikacioni broj, podataka o lokaciji, identifikatora u elektronskim komunikacionim mrežama ili jednog, odnosno više obeležja njegovog fizičkog, fiziološkog, genetskog, mentalnog, ekonomskog, kulturnog i društvenog identiteta".[13] Lice za zaštitu podataka o ličnosti (engl. *Data Protection Officer*) predstavlja pravni institut koji je „uveden u domaće pravo kao primer dobre prakse evropskog zakonodavstva i evropske prakse"[14], a poseduje „prevashodno konsultativnu, edukacionu i usmeravajuću funkciju"[15], budući da mu je zadatak da „pomaže u radu organizacije ili licu kod koga je imenovano"[16] i „pomaže da smanji rizike i prilagodi svoje delovanje novim standardima privatnosti"[17]. Međutim, iako ZZPL previđa obavezu za kompanije odrede lice za zaštitu podataka o ličnosti, mali broj kompanija je to i učinio[18].

Sa druge strane, sve do 2004. godine korporativno upravljanje skoro da je bilo nepoznanica srpskom pravu[19], a prvi Kodeks korporativnog upravljanja usvojen je 2005. godine.[20] Trenutno važeći Kodeks korporativnog upravljanja donet je 2012. godine od strane Privredne komore Srbije[21]. Budući da je Kodeks donet šest godina pre stupanja na snagu GDPR i ZZPL, ne iznenađuje činjenica da se zaštita podataka o ličnosti nigde ne spominje.

Značaj zaštite podataka o ličnosti svakim danom sve više raste, uzimajući u obzir vrednost informacija o korisnicima, kao i moguće zloupotrebe. Kompanije sakupljaju podatke o ličnosti svojih korisnika kako bi im obezbedile bolje iskustvo i pružile bolje usluge. Postavlja se pitanje šta se dešava sa tim

---

[13] Član 4(1) Zakona o zaštiti podataka o ličnosti, *Sl. glasnik RS*, br. 87/2018.

[14] S. Andonović, „Lice za zaštitu podataka o ličnosti u pravnom sistemu Srbije", u: *Zaštita podataka o ličnosti u Srbiji: zbornik radova* (ur. S. Andonović, D. Prlja, A. Diligenski), Institut za uporedno pravo, Beograd 2020, 118.

[15] *Ibid*.

[16] *Ibid*.

[17] *Ibid*., 127.

[18] T. Žunić Marić, J. Đukanović, Data Protection Officer vs Country Representative for Serbia, https://zuniclaw.com/en/data-protection-officer-serbia/, posećeno: 30. 3. 2025.

[19] V. Radović, O približavanju Kodeksa korporativnog upravljanja zakonskoj regulativi, *Teme* 40(2016)3, 1128.

[20] *Službeni glasnik RS*, br. 1/2006.

[21] Kodeks korporativnog upravljanja, *Sl. glasnik RS,* br. 99/2012.

podacima, gde se oni pohranjuju, kako i na koji način se koriste i obrađuju, ko ima pristup tim podacima i u koje svrhe. Pored toga, u prilog neophodnosti regulisanja ove materije govori i činjenica da je predviđena krivičnopravna odgovornost za mnoge vidove zloupotrebe podataka o ličnosti[22].

S tim u vezi, važno je objasniti pojam *kompromitacija podataka.* Kompromitacija podataka (engl. *data breach*) definiše se kao „bezbednosni incident u kome se osetljivi, zaštićeni ili poverljivi podaci kopiraju, prenose, gledaju, kradu ili koriste od strane pojedinca koji je neovlašćen za pristup tim podacima"[23]. Može se reći da kompromitacija podataka predstavlja najčešću povredu podataka o ličnosti.

III Zaštita podataka o ličnosti kao zadatak korporativnog upravljanja

Dobro korporativno upravljanje u direktnoj je vezi sa zaštitom podataka o ličnosti, budući da se zasniva na principima transparentnosti[24], dužnosti i odgovornosti[25]. Ovakva veza je već uveliko prepoznata u stranoj literaturi i praksi[26]. Izmene nemačkog Kodeksa korporativnog upravljanja iz 2017. godine fokusiraju se na usklađenost poslovanja i zaštite podataka o ličnosti, a određeni autori su već govorili o značaju i povezanosti GDPR-a i usklađenosti poslovanja[27]. Pored toga, u Japanu se uveliko ističe značaj lica za zaštitu podataka o ličnosti

[22] Vidi Lj. Slijepčević, Privatnost i zaštita podataka o ličnosti kroz domaće i međunarodno pravo s osvrtom na korisnike Fejsbuka i interneta sa krivičnopravnog aspekta, https://pars.rs/public/Dokumenti/Publikacije/1508/Privatnost-i-zastita-podataka-o-licnosti-kroz-domace-i-medjuanrodno-pravo.pdf, posećeno: 30. 3. 2025.

[23] G. Matić, Osnove obrade i zaštite podataka – priručnik, https://nsa.gov.rs/extfile/sr/1424/Osnove_obrade_i_zastite_podataka-prirucnik.pdf, 93, posećeno: 29. 3. 2025.

[24] A. Tan, Emerging stronger together with co-ops – strengthening personal data protection and corporate governance, https://www.mccy.gov.sg/about-us/news-and-resources/speeches/2021/jul/emerging-stronger-together-with-co-ops, posećeno: 24. 3. 2025.

[25] S. Kusumawardani, S. D. Rosadi, E. Gultom, Good corporate governance principles on internet intermediary companies in protecting the privacy of personal data in Indonesia, *Yustisia Jurnal Hukum* 9(2020)1, 66.

[26] C. Ritzer, Cyber risk and directors' liabilities: an international perspective, 2016, https://www.nortonrosefulbright.com/en/knowledge/publications/b0dae4a0/cyber-risk-and-directors-liabilitiesan-international-perspective, posećeno: 26. 5. 2025.

[27] H.P. Marutschke, New Developments in German Corporate Governance Law with Focus on Compliance and Data Protection Issues (GDPR), *Doshisha Law Review* 71(2019)1, 89–90.

za korporativno upravljanje[28], dok je u američkoj pravnoj teoriji prisutan ekstenzivan broj radova na temu sajber bezbednosti i odgovornosti direktora.

1. Sajber bezbednost kao novi rizik poslovanja

Sajber bezbednost, kao jedan od najvažnijih rizika poslovanja u digitalnom dobu, i dobro korporativno upravljanje, kao način efikasnog upravljanja rizicima poslovanja, neraskidivo su povezani. Kada se govori o ESG (engl. *Environmental, Social and Governance*) standardima, ističe se da sajber bezbednost i zaštita podataka predstavljaju značajne rizike upravljanja kompanija[29]. Pored toga, neki autori tvrde da je „zaštita podataka podskup sajber bezbednosti"[30].

Sajber bezbednost (engl. *cybersecurity*) se može ukratko definisati kao „praksa zaštite digitalnih informacija, uređaja i resursa"[31]. Ekstenzivno definisanje sajber bezbednosti sugeriše da ona predstavlja „zaštitu računarskih sistema i mreža od napada zlonamernih aktera koji mogu dovesti do neovlašćenog otkrivanja informacija, krađe ili oštećena hardvera, softvera ili podataka"[32]. Pojmovi računarska bezbednost, digitalna bezbednost ili bezbednost informacionih tehnologija (IT bezbednost) predstavljaju sinonime za termin sajber bezbednost[33].

Pored toga, *sajber bezbednosni rizici* (engl. *cybersecurity risks*) „odnose se na gubitak poverljivosti, integriteta ili dostupnosti informacija, podataka ili informacionih (ili kontrolnih) sistema i odražavaju potencijalne negativne posledice na organizacione operacije (tj. misiju, funkcije, imidž ili reputaciju), imovinu, pojedince, druge organizacije i naciju"[34]. S tim u vezi, cilj sajber be-

---

[28] Ministry of Internal Affairs and Communications, Ministry of Economy, Trade and Industry of Japan, *op. cit.*, 24–27, 33–37.

[29] W. Tan, B. Guo, Q. Zhang, Cybersecurity governance and corporate market value: Perspectives from investor trust and supply chain trust, *Pacific-Basin Finance Journal* 90(2025), 1.

[30] P. Tester, Cybersecurity & Data Protection—Key Differences & Benefits, https://datadome.co/learning-center/cybersecurity-and-data-protection/, posećeno: 26. 3. 2025.

[31] Šta je kibernetička bezbednost?, https://support.microsoft.com/sr-latn-rs/topic/%C5%A1ta-je-sajber-bezbednost-8b6efd59-41ff-4743-87c8-0850a352a390, posećeno: 29. 3. 2025.

[32] G. Matić, *op. cit.*

[33] *Ibid.*

[34] Share fondacija, Procena rizika od sajber prednji, 2023, https://sharefoundation.info/procena-rizika-od-sajber-pretnji/, posećeno: 29. 3. 2025.

zbednosti „jeste da smanji rizike od sajber napada i zaštiti od neovlašćenog iskorišćavanja sistema, mreže i tehnologije"[35].

Dakle, upravo putem sajber napada i dolazi do kompromitacije podataka, kao jednog od najčešćih oblika povreda podataka o ličnosti. Kompanije su često na meti sajber napada, a samim tim su izložene riziku kompromitacije podataka. Budući da kompromitacija podataka može imati dalekosežne posledice na poslovanje kompanije, jasno je zašto se fokus sve više okreće ka umanjivanju sajber bezbednosnih rizika.

Stručnjaci ističu da je sajber bezbednost „prepoznata kao ključni element korporativne strategije i upravljanja rizikom"[36]. U današnjem digitalnom dobu smatra se da „integracija sajber bezbednosti u korporativno upravljanje više nije samo strateški izbor već fundamentalna neophodnost"[37], i da se „kritičnost sajber bezbednosti u domenu korporativnog upravljanja ne može preceniti"[38]. Takođe, ističe se da je adekvatno korporativno upravljanje „ključno za ublažavanje rizika, reagovanje na incidente u sajber bezbednosti i demonstriranje spremnosti"[39].

O značaju sajber bezbednosti za korporativno upravljanje takođe govori i činjenica da su kompanije kotirane na američkoj berzi u obavezi da Komisiji za hartije od vrednosti SAD dostavljaju detaljne godišnje izveštaje o upravljanju sajber bezbednosnim rizicima, uključujući izveštaje o nadzoru direktora nad upravljanjem sajber bezbednosnim rizicima, kao i posebne izveštaje o eventualnim incidentima u vezi sa sajber bezbednošću[40].

Pravne regulative i pravni propisi su od velikog značaja za korporativno upravljanje sajber bezbednosnim rizicima[41], ali, takođe, neophodno je da se

---

[35] G. Matić, *op. cit.*

[36] T. Mumtaz Awan, Z. Riaz Pitafi, "Perspective Chapter: Cybersecurity and Risk Management – New Frontiers in Corporate Governance", in: *Corporate Governance - Evolving Practices and Emerging Challenges* (ed. T. Mumtaz Awan), IntechOpen, London 2024, 4.

[37] *Ibid.*, 1.

[38] *Ibid.*, 2.

[39] O. Cox, H. Kanji, Building Effective Cybersecurity Governance, 2022, https://corpgov.law.harvard.edu/2022/11/10/building-effective-cybersecurity-governance/, posećeno: 30. 3. 2025.

[40] B. George, C. Lyon, P. Marcogliese, Data in the Driver's Seat: What Boards Need to Know about Data Governance, 2024, https://corpgov.law.harvard.edu/2024/04/30/data-in-the-drivers-seat-what-boards-need-to-know-about-data-governance/, posećeno: 26. 3. 2025.

[41] W. Tan, B. Guo, Q. Zhang, *op. cit.*, 3.

kompanije na internom i eksternom planu prilagode novim potrebama zaštite podataka o ličnosti.

2. Unutrašnja struktura kompanije i zaštita podataka o ličnosti

Kada se govori o sajber bezbednosti, važno je naglasiti da adekvatna prevencija i zaštita podrazumevaju „dugoročan pristup u cilju postizanja inkrementalnih poboljšanja bezbednosti i zaštite promenom organizacione kulture"[42].

Slučajevi sajber napada i kompromitacije podataka mogu dovesti do gubitka podataka o ličnosti[43], a ovakvi slučajevi su sve češći u praksi[44]. Ekonomske posledice narušavanja sajber bezbednosti zavise od prirode i vrednosti zaštićenog dobra[45] (u ovom slučaju, podataka o ličnosti), i mogu dovesti do značajnih finansijskih gubitaka (kazne, odštete, troškovi suđenja) i reputacionih gubitaka.

Problematika kompromitacije podataka može biti vrlo skupa i može imati mnogo negativnih posledica po reputaciju same kompanije[46] – u praksi direktori neretko bivaju smenjeni nakon sajber napada – a takođe se negativno odražava na prinos akcija u narednoj godini poslovanja[47].

Pregled literature i istraživanja u prvoj deceniji 21. veka pokazuje da se, čak i tad, kompromitacija podataka u određenim kompanijama negativno odražavala na vrednost akcija tih kompanija[48]. Takođe, pokazano je da su akcionari

[42] H. Lehuedé, Corporate governance and data protection in Latin America and the Caribbean, *Production Development series, No. 223 (LC/TS.2019/38)*, Santiago, Economic Commission for Latin America and the Caribbean (ECLAC), 2019, 23.

[43] S. W. Klemash, J. C. Smith, C. Seets, What Companies are Disclosing About Cybersecurity Risk and Oversight, 2020, https://corpgov.law.harvard.edu/2020/08/25/what-companies-are-disclosing-about-cybersecurity-risk-and-oversight/, posećeno: 24. 3. 2025.

[44] L. A. Aguilar, Boards of Directors, Corporate Governance and Cyber-Risks: Sharpening the Focus, Cyber Risks and the Boardroom Conference, New York Stock Exchange 2014, https://www.sec.gov/newsroom/speeches-statements/2014-spch061014laa, posećeno: 24. 3. 2025.

[45] K. Campbell *et al*., The economic cost of publicly announced information security breaches: empirical evidence from the stock market, *Journal of Computer Security* 11(2003)3, 445.

[46] C. Lending, K. Minnick, P. J. Schorno, Corporate Governance, Social Responsibility, and Data Breaches, *The Financial Review* 53(2018)2, 420.

[47] *Ibid*., 450-451.

[48] K. M. Gatzlaff, K. A. McCullough, The effect of data breaches on shareholder wealth, *Risk Management and Insurance Review* 13(2010)1, 65, 75; S. Goel, H. A. Shawky, Estimating the

i zainteresovane strane (tzv. stejkholderi) prihvatali određene rizike poslovanja, ali su već tada bili obazriviji kada su u pitanju poverljive informacije i podaci o ličnosti[49].

Neki autori smatraju da je zaštita podataka o ličnosti jedan od ključnih problema na koji se direktori moraju fokusirati kako bi se ublažili rizici i da to predstavlja njihovu fiducijarnu dužnost[50]. Drugi autori odlaze korak dalje u svojim tvrdnjama i navode da dobro korporativno upravljanje može smanjiti šanse da kompanija bude meta sajber napada[51]. Takođe, isti autori tvrde da kompanije sa boljim korporativnim upravljanjem češće ulažu u resurse potrebne za prevenciju sajber napada[52].

Takođe, ističe se da „upravljanje sajber bezbednošću doprinosi izgradnji usaglašene, bezbedne i efikasne korporativne kulture, pružajući snažnu stratešku podršku za povećanje tržišne vrednosti"[53], kao i da takva korporativna kultura „jača poverenje zainteresovanih strana u kompaniju, poboljšava društveno priznanje i dalje unapređuje tržišnu konkurentnost, dovodeći do povećanja tržišne vrednosti"[54].

Smatra se da sajber bezbednost zapravo predstavlja odgovornost svih direktora[55], a to zahteva određeni stepen stručnosti i poznavanja materije.

---

market impact of security breach announcements on firm values, *Information & Management* 46(2009)7, 406–408.

[49] K. Campbell *et al., op. cit.,* 436.

[50] M. E. Wanja, Governance in the data age:the application of corproate governance to ensure consumer data protection in Kenya, master thesis, University of Nairobi, 2019, https://erepository.uonbi.ac.ke/bitstream/handle/11295/108799/Mugo_Governance%20in%20the%20Data%20Age-%20the%20Application%20of%20Corporate%20Governance%20to%20Ensure%20Consumer%20Data%20Protection%20in%20Kenya.pdf?sequence=1&isAllowed=y, 92, posećeno: 19. 3. 2025; C. C. Hartmann, J. Carmenate, Academic Research on the Role of Corporate Governance and IT Expertise in Addressing Cybersecurity Breaches: Implications for Practice, Policy, and Research, *Current Issues in Auditing* 15(2011)2, A20.

[51] C. Lending, K. Minnick, P. J. Schorno, *op. cit.,* 414-415.

[52] *Ibid.*, 417.

[53] W. Tan, B. Guo, Q. Zhang, *op. cit.*, 4.

[54] *Ibid.*

[55] S. Conmy, A cyber security guide for board members, https://www.thecorporategovernanceinstitute.com/insights/guides/cyber-security-guide-board-members/?srsltid=AfmBOorV3WxQusIP5HDr3lSBy7K5d2S_DzMuHdT4_-Sna4_WQ0Sgde86, posećeno: 26. 3. 2025;

Kada se govori o stručnosti direktora, oportuno bi bilo da direktori poseduju finansijsku stručnost, budući da bi takva lica bila svesnija finansijskih posledica po kompaniju u slučaju kompromitacije podataka . Isto tako, činjenica je da direktori ne poseduju dovoljno znanja iz oblasti sajber bezbednosti, te se preporučuju kontinuirane edukacije direktora, koje su neke kompanije već uvele[56]. Zapravo, ovakva vrsta edukacije direktora predstavlja ključni element procesa integracije sajber bezbednosti u korporativno upravljanje[57].

3. Interni i eksterni mehanizmi upravljanja zaštitom podataka o ličnosti

Pored kontinuirane edukacije direktora (ali i zaposlenih u kompaniji) u oblasti sajber bezbednosti, postoje i drugi načini na koje kompanije manevrišu sajber bezbednosne rizike. Postoje različiti načini na koje kompanije mogu da se zaštite od hakerskih napada, a uzimajući u obzir značaj zaštite podataka za poslovanje kompanije, čak su zabeleženi i slučajevi konsultacija sa etičkim, tzv. „belim" hakerima[58].

Takođe, istraživanja pokazuju da su kompanije već počele da formiraju posebne IT odbore unutar svoje strukture, sa ciljem ublažavanja rizika informacionih tehnologija i drugih rizika u vezi sa zaštitom podataka, a neke kompanije ove zadatke poveravaju odborima za reviziju ili odvojenim odborima za procenu rizika[59]. Budući da je sajber bezbednost od velike važnosti za korporativno upravljanje, jača i uloga odbora za reviziju u cilju „premošćavanja jaza između tehničkog IT jezika i zahteva finansijskog izveštavanja i poboljšanja transparentnosti u upravljanju sajber bezbednosnim rizicima, kako bi se ispunili regulatorni standardi"[60].

Ministry of Internal Affairs and Communications, Ministry of Economy, Trade and Industry of Japan, *op. cit.*, 21–22.

[56] E. F. Pérez Carrillo, Cybersecurity in European Financial Institutions: New Grounds for Corporate Governance Reform, *European Business Law Review* 34(2023)7, 1158; A. Tan, *op. cit.*; S. W. Klemash, J. C. Smith, C. Seets, *op. cit.*

[57] T. Mumtaz Awan, Z. Riaz Pitafi, *op. cit.*, 6.

[58] S. Singh, V. Upreti, Corporate Governance and Cyber Security, *International Journal of Law Management & Humanities* 4(2021)4, 2812–2813, 2816.

[59] C. C. Hartmann, J. Carmenate, *op. cit.*, A13-A15; S. W. Klemash, J. C. Smith, C. Seets, *op. cit*.

[60] Z. Guohong *et al.*, The Audit Committee's IT Expertise and Its Impact on the Disclosure of Cybersecurity Risk, *Research in International Business and Finance* 73(2025), 2.

Tako, smatra se da „članovi odbora za reviziju koji su stručni u IT oblasti mogu sveobuhvatnije razumeti prirodu sajber rizika, identifikovati potencijalne tehničke „slabe tačke" i razumeti kako one mogu uticati na finansijsku i operativnu stabilnost kompanije"[61].

Pored ovih mehanizama, važno je istaći značaj lica za zaštitu podataka o ličnosti[62]. Autori koji zagovaraju model korporativnog upravljanja koji je okrenut zaštiti podataka o ličnosti, ističu da je cilj takvog modela korporativnog upravljanja upravo usklađenost poslovanja kompanije sa regulativom zaštite podataka o ličnosti, uz zaštitu interesa ostalih zainteresovanih strana[63]. Upravo jedan od krucijalnih elemenata takvog modela jeste lice za zaštitu podataka o ličnosti, čiji je zadatak da obezbedi „razumnu proporcionalnost između interesa i prava korporacija"[64].

Kao jedna od ključnih osobina lica za zaštitu podataka o ličnosti ističe se njegova nezavisnost od ostalih organa, a zabeleženi su i slučajevi plaćanja visokih kazni od strane kompanija za nepoštovanje ili dovođenje u pitanje njegove nezavisnosti.[65]

Potreba za licem koje poseduje specijalizovana znanja iz oblasti sajber bezbednosti i informacionih tehnologija je postala evidentna, te se u praksi u nekim kompanijama javlja direktor za bezbednost informacija (engl. C*ISO – Chief Information Security Officer*)[66]. Njegovi zadaci obuhvataju razvijanje i sprovođenje strategije sajber bezbednosti, nadgledanje bezbednosti informacija i vršenje procene rizika.[67]

---

[61] *Ibid*., 3.

[62] Ministry of Internal Affairs and Communications, Ministry of Economy, Trade and Industry of Japan, *op. cit*., 24–27, 33–37; S. W. Klemash, J. C. Smith, C. Seets, *op. cit*.; A. Diligenski, D. Prlja, D. Cerović, *Pravo zaštite podataka GDPR*, Institut za uporedno pravo, Beograd 2018, 191–205.

[63] A. Tokhadze, The Interdisciplinary Analysis of Institutional Role of Data Protection Officer in the System of Corporate Governance, *Journal of Personal Data Protection Law* (2023)1, 109.

[64] *Ibid*., 107.

[65] E. F. Pérez Carrillo, *op. cit*., 1162–1163, fn. 78–81.

[66] K. Machilsen, E. Haedens, Why cybersecurity should be a board priority, https://www.ey.com/en_be/insights/cybersecurity/why-cybersecurity-should-be-a-board-priority#:~:text=Therefore%2C%20boards%20must%20prioritize%20cybersecurity,and%20training%20as%20key%20components, posećeno: 24. 3. 2025.

[67] P. Monzelo, S. Nunes, "The Role of the Chief Information Security Officer (CISO) in Organizations", in: *19.ª Conferência da Associação Portuguesa de Sistemas de Informação (CAPSI'2019)*, 2019, 3–4 i dalje.

Dakle, krucijalna razlika između ova dva lica odnosi se na objekat zaštite – direktor za bezbednost informacija ima zadatak da vodi računa o interesima kompanije, a lice za zaštitu podataka o ličnosti ima zadatak da vodi računa o interesima zainteresovanih strana[68]. Samim tim, direktor za bezbednost informacija može biti deo izvršnog odbora, a lice za zaštitu podataka o ličnosti to nikako ne sme biti.

Interni i eksterni mehanizmi, kao i edukativne strategije unutar kompanija, predstavljaju načine na koje kompanije pokušavaju da umanje sajber bezbednosne rizike i time izbegnu katastrofalne posledice po svoje poslovanje. Međutim, praksa poslednjih godina pokazuje da su sajber incidenti postali izuzetno česti, a odgovori kompanija na iste se smatraju, u najmanju ruku, krajnje neadekvatnim.

IV (Ne)transparentnost kompanija prilikom kompromitacije podataka o ličnosti

Neki autori sugerišu da je sajber napad u određenoj kompaniji prilika za ostale kompanije da postanu svesne stvarnih ili percipiranih sajber bezbednosnih rizika u svom poslovanju[69]. Tako, pravi se razlika između *stvarnog rizika*, odnosno novih „slabih tačaka" poslovanja, kojih, do sajber napada, druge kompanije nisu bile svesne, i *percipiranog rizika*, odnosno „slabih tačaka" kojih su druge kompanije bile svesne, ali su zanemarivale njihov značaj[70]. Takođe, istraživanja su pokazala da kompromitacija podataka može dovesti do poboljšanja unutrašnjih kontrola u drugim kompanijama, pri čemu se može zaključiti da sajber napadi implicitno utiču i na korporativno upravljanje[71].

Dakle, posmatrajući sa pozitivne strane, sajber napadi mogu biti prilika i za pogođene kompanije, ali i za i ostale kompanije da unaprede svoje korporativno upravljanje, budući da (kompanije) tada postaju svesne novih sajber bezbednosnih rizika, i imaju mogućnost da adekvatnije usklade svoje poslovanje i upravljanje rizicima. Svojim delovanjem, bilo preventivnim ili postven-

[68] DPO Associates, The DPO and the CISO: what is the difference between the two positions?, https://dpoassociates.eu/en/the-dpo-and-the-ciso-what-is-the-difference-between-the-two-positions/, posećeno: 24. 3. 2025.

[69] M. Ashraf, The Role of Peer Events in Corporate Governance: Evidence from Data Breaches, *The Accounting Review* 97(2022)2, 5.

[70] *Ibid.*

[71] *Ibid.*, 19.

tivnim, kompanije imaju šansu da preduprede buduće sajber napade i time podignu svoju sajber bezbednost na viši nivo.

Posmatrano u realnom svetu, sajber napadi i kompromitacija podataka predstavljaju sve osim „dobrih prilika" za kompanije. Kada se analiziraju odnos transparentnosti poslovanja društva i zaštite podataka o ličnosti, evidentno je da kompromitacija podataka povlači sa sobom brojne negativne posledice za kompaniju, kako finansijske, tako i reputacione. Stoga je neophodno da akcionari i zainteresovane strane imaju poverenje u spremnost kompanije da zaista obezbedi adekvatnu zaštitu podataka, kao i da se odbrani od potencijalnih sajber napada, a to poverenje se stiče transparentnošću poslovanja i znanjem kako i na koji način direktori upravljaju takvim rizicima[72]. Pored toga, zabeleženi su i slučajevi proaktivnog delovanja akcionara povodom ovih pitanja[73], imajući u vidu značaj zaštite podataka, kao i posledice sajber napada.

Kada se govori o korporativnom upravljanju u kontekstu zaštite podataka o ličnosti i sajber bezbednosti, odnosno neadekvatnoj reakciji menadžmenta u slučaju kompromitacije podataka, očigledno je da dolaze do izražaja informaciona asimetrija i agencijski problemi[74]. Ako do kompromitacije podataka zaista dođe, neophodno je da kompanija obavesti o događaju, kako direktore, akcionare i zainteresovane strane, tako i samu javnost, i preuzme odgovornost za neadekvatno upravljanje rizicima, što je u skladu sa transparentnošću poslovanja. Budući da sajber bezbednosni rizici sa sobom povlače značajne posledice, neophodno je da kompanije učine sve u njihovoj moći da sajber napade spreče. Međutim, u poslednjoj deceniji zabeleženo je više desetina slučajeva u kojima su kompanije želele da zataškaju takve incidente, što se kasnije pokazalo kao izuzetno loša odluka menadžmenta, sa brojnim negativnim posledicama, kako po samu kompaniju, tako i po odgovorna lica u kompaniji.

1. Studija slučaja

U kompaniji *Altbama* (nekadašnji *Yahoo! Inc.*) se 2014. godine dogodio jedan od najvećih sajber napada, prilikom kojeg su ukradeni podaci više stotina miliona korisnika. Ti podaci su obuhvatali korisnička imena, adrese elektronske

[72] S. W. Klemash, J. C. Smith, C. Seets, *op. cit.*

[73] *Ibid.*

[74] E. K. Cortez, M. Dekker, A Corporate Governance Approach to Cybersecurity Risk Disclosure, *European Journal of Risk Regulation (EJRR)* 13(2022)3, 445. Vidi i W. Tan, B. Guo, Q. Zhang, *op. cit*., 5 i dalje.

pošte, lozinke, odgovore na sigurnosna pitanja, datume rođenja, itd. Iako su menadžment i pravno odeljenje bili obavešteni, kompanija je pokušala da zataška incident, prećutavši investitorima i revizorima činjenicu da je došlo do sajber napada, da bi se događaj obelodanio tek dve godine kasnije, prilikom akvizicije od strane kompanije *Verizon Communications*, *Inc.*. Na kraju je Komisija za hartije od vrednosti SAD objavila da je kompanija *Altbama* u obavezi da plati kaznu u iznosu od 35 miliona američkih dolara za obmanjivanje investitora[75].

Kompanija *Facebook, Inc.* je tokom 2014. i 2015. godine omogućila kompaniji za obradu podataka *Cambridge Analytica* da kreira test ličnosti i analizira rezultate skoro 30 miliona američkih korisnika. Međutim, *Cambridge Analytica* je pored rezultata testa neovlašćeno prikupljala i obrađivala i druge podatke o ličnosti korisnika, uključujući podatke o imenima, polu, uzrastima, datumima rođenja, lokacijama korisnika i njihovim online aktivnostima na popularnoj društvenoj mreži (tzv. „sviđanja" objava), u cilju adekvatnijeg reklamiranja političkih aktivnosti. Iako je izvesno da je kompanija *Facebook, Inc.* postala svesna incidenta tokom 2015. godine, incident je ostao zataškan naredne dve godine, a investitorima je samo sugerisana mogućnost neadekvatne obrade podataka. Pored toga, kompanija je poricala da je došlo do kompromitacije podataka, a samim tim je obmanjivala i novinare koji su istraživali slučaj. Cena akcija kompanije je pala nakon što je kompanija objavila da je ipak došlo do incidenta. Ne priznajući niti poričući, kompanija je pristala da plati kaznu od 100 miliona američkih dolara[76].

Sa druge strane, zanimljiv je i slučaj kompanije *Equifax*. Naime, kompanija *Equifax* pretrpela je hakerski napad navodno krajem jula 2017. godine, kada je došlo do kompromitacije podataka oko 147 miliona korisnika, ali je odlučila da privremeno zataška incident, i izvestila je o istom tek početkom septembra 2017. godine. U roku od nedelju dana od izveštavanja javnosti o incidentu cena akcija kompanije je pala za neverovatnih 32%. Međutim, kako je kasnija istraga pokazala, direktori u kompaniji su postali svesni sajber napada već u martu 2017. godine, i od marta 2017. godine do septembra 2017. godine većina direktora je prodala svoje akcije kompanije, a nakon izveštavanja o incidentu

[75] SEC, Altaba, Formerly Known as Yahoo!, Charged With Failing to Disclose Massive Cybersecurity Breach; Agrees To Pay $35 Million, 2018, https://www.sec.gov/newsroom/press-releases/2018-71, posećeno: 24. 3. 2025.

[76] SEC, Facebook to Pay $100 Million for Misleading Investors About the Risks It Faced From Misuse of User Data, 2019, https://www.sec.gov/newsroom/press-releases/2019-140, posećeno: 24. 3. 2025.

podneli su ostavke (uključujući finansijskog direktora, direktora informacionih tehnologija i generalnog direktora)[77]. Čak je napravljen i poseban veb sajt u cilju lakšeg obaveštavanja javnosti o toku nagodbe i isplati oštećenih lica u iznosu između 400 i 500 miliona američkih dolara[78]. Pored toga, kompanija je morala da plati kazne u iznosu o 275 miliona američkih dolara[79]. Dakle, ukupne finansijske kazne koje je kompanija *Equifax* morala da plati iznose preko 700 miliona američkih dolara, a bivši direktori kompanije su osuđeni na kazne zatvora zbog trgovanja na osnovu insajderskih informacija[80].

Kompanija *Uber* pretrpela je sajber napad 2016. godine, kada su ukradeni podaci preko 57 miliona korisnika i vozača, uključujući lične podatke, kao i brojeve vozačkih dozvola vozača. Kompanija je želela da zataška incident i pristala je da plati hakerima 100 hiljada dolara da unište ukradete podatke, a izvestila je javnost o incidentu i plaćanju tek 2017. godine. Federalna trgovinska komisija SAD je kaznila kompaniju *Uber* u visini od 148 miliona američkih dolara (dakle, 1,480 puta veći iznos nego što su platili hakerima), a iste godine kompanija je zaposlila nova lica kako bi nadgledali poštovanje politike privatnosti[81].

Krađa podataka može biti vrlo rizična, uzimajući u obzir činjenicu da je, na primer, u 2019. godini u Indoneziji zabeleženo više slučajeva kompromitacije podataka desetina miliona korisnika kompanija *PT Bukalapak* i *Malindo Air*, da bi se ti podaci kasnije ilegalno prodavali na tzv. *dark web*-u[82]. Pored ovih slučajeva, u 2024. godini zabeležen je i slučaj kompromitacije podataka u američkoj kompaniji *Dell Technologies*, kada su hakeri ukrali podatke o ličnosti skoro 49

---

[77] H. Grove, M. Clouse, L. G. Schaffner, Cybersecurity description and control criteria to strengthen corporate governance, *Journal of Leadership, Accountability and Ethics* 16(2019)1, 88.

[78] https://www.equifaxbreachsettlement.com/, posećeno: 27. 3. 2025.

[79] FTC, Equifax to Pay $575 Million as Part of Settlement with FTC, CFPB, and States Related to 2017 Data Breach, 2019, https://www.ftc.gov/news-events/news/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related-2017-data-breach, posećeno: 27. 3. 2025.

[80] U.S. Attorney's Office, Northern District of Georgia, Former Equifax employee sentenced for insider trading, 2019, https://www.justice.gov/usao-ndga/pr/former-equifax-employee-sentenced-insider-trading, posećeno: 27. 3. 2025.

[81] S. A. O'Brien, Uber to pay record $148 million over 2016 data breach, 2018, https://money.cnn.com/2018/09/26/technology/uber-settlement-data-breach/index.html?section=money_technology, posećeno: 29. 3. 2025.

[82] S. Kusumawardani, S. D. Rosadi, E. Gultom, *op. cit.*, 67–81.

miliona korisnika, a kompanija je pokušala da umanji značaj incidenta ističući da nisu ukradeni finansijski podaci korisnika. Kasnije su se ovi podaci takođe ilegalno prodavali na tzv. *dark web*-u[83].

Kada analiziramo nabrojane slučajeve, vidimo da su kompromitovani podaci o ličnosti korišćeni u različite svrhe – od adekvatnijeg targetiranja korisnika političkim reklamnim kampanjama, preko ucenjivanja kompanijama ukradenim podacima, do ilegalne prodaje podataka putem interneta. Ovi slučajevi takođe govore u prilog činjenici da su, u današnjem svetu informacija, podaci o ličnosti korisnika od izuzetnog značaja, a nažalost poseduju čak i tržišnu vrednost.

Isto tako, kompromitacija podataka i na tržišnu vrednost akcija pogođenih kompanija, u tolikoj meri da direktori odlažu obelodanjivanje incidenata kako bi umanjili svoje gubitke na račun akcionara i zainteresovanih strana. Stoga ne iznenađuju postupci i napori kompanija da na svaki mogući način zataškaju sajber napade i kompromitaciju podataka.

2. Povrede članova GDPR-a

Kompanije koje posluju na teritoriji EU u obavezi su da poštuju odredbe GDPR-a[84]. Međutim, zabeleženo je mnogo slučajeva povreda članova GDPR-a, među kojima se najviše ističu slučajevi kompanije *Facebook, Inc.* i kompanije *Amazon*. Naravno, važno je napomenuti da ni druge kompanije nisu ostale imune na primenu GDPR-a[85].

Kompanija *Facebook, Inc.* imala je brojne incidente u vezi nepoštovanjem članova GDPR-a, pogotovo u Irskoj. Tako, tokom 2018. godine, ukradeni su podaci blizu 29 miliona korisnika, uključujući podatke o imenima i prezimenima, veroispovesti, polu, datumima rođenja, adresama, brojevima telefona, adresama elektronske pošte, radnim mestima, itd. Prema saopštenju irske Komisije za zaštitu podataka, kompanija *Meta* (kompanija-majka kompanije

[83] T. Claburn, Dell customer order database of '49M records' stolen, now up for sale on dark web, 2019, https://www.theregister.com/2024/05/09/dell_data_stolen/, posećeno: 28. 3. 2025.

[84] C. Tikkinen-Piria, A. Rohunena, J. Markkula, EU General Data Protection Regulation: Changes and implications for personal data collecting companies, *Computer Law & Security Review* 34(2017)1, 2.

[85] Data Privacy Manager, 20 biggest GDPR fines so far, 2025, https://dataprivacymanager.net/5-biggest-gdpr-fines-so-far-2020/, posećeno: 29. 3. 2025.

Facebook, Inc.) je morala da plati kaznu u iznosu od 251 miliona evra, za nepoštovanje odredaba GDPR-a[86]. Pored ove kazne, kompanija *Meta* je tokom 2022. godine u više navrata morala da plati irskoj Komisiji za zaštitu podataka kazne za povrede preko deset odredaba GDRP-a u ukupnom iznosu od 687 miliona evra, tokom 2024. godine „samo" 342 miliona evra[87]. Međutim, ono što je zapanjujuće jeste podatak da je u 2023. godini kompanija *Meta*, zbog neusklađenosti poslovanja sa odredbama GDPR-a i transfera podataka o ličnosti evropskih korisnika u SAD, kažnjena od strane irske Komisije za zaštitu podataka u iznosu od čak 1,2 milijardi evra[88]! Ova kazna predstavlja najvišu do sad izrečenu kaznu za povredu GDPR-a.

Iako kompanija *Meta* ubedljivo prednjači kada su u pitanju povrede GDPR-a i visine plaćenih kazni, počasno drugo mesto pripada kompaniji *Amazon*. Naime, kompanija *Amazon* je tokom 2018. godine neovlašćeno, odnosno bez saglasnosti korisnika, sakupljala podatke o ličnosti korisnika u cilju oglašavanja. Luksemburška Nacionalna komisija za zaštitu podataka je odredila kaznu u iznosu od 746 miliona evra. U martu 2025. godine doneta je presuda luksemburškog suda kojom se potvrđuje odluka Nacionalne komisije za zaštitu podataka, a kompaniji *Amazon* ostaje da odluči da li će se žaliti na presudu[89].

Pored kompanija *Meta* i *Amazon*, mnoge velike kompanije su takođe bile kažnjene od strane nadležnih organa za povrede ili nepoštovanje odredaba GDPR-a: kompanija *Tik Tok* je 2023. godine bila obavezna da plati kaznu u iznosu od 345 miliona evra[90], kompanija *LinkedIn* je u 2024. godini kažnjena u iznosu od 310 miliona evra[91], kompanija *Google* u 2021. godini je kažnjena

---

[86] Data Protection Commission, Irish Data Protection Commission fines Meta €251 Million, 2024, https://www.dataprotection.ie/en/news-media/press-releases/irish-data-protection-commission-fines-meta-eu251-million, posećeno: 28. 3. 2025.

[87] https://www.enforcementtracker.com/, posećno: 28. 3. 2025.

[88] European Data Protection Board, 1.2 billion euro fine for Facebook as a result of EDPB binding decision, 2023, https://www.edpb.europa.eu/news/news/2023/12-billion-euro-fine-facebook-result-edpb-binding-decision_en, posećeno: 28. 3. 2025.

[89] C. Kroet, Amazon considers appeal after court sides with regulator on record privacy fine, 2025, https://www.euronews.com/next/2025/03/20/amazon-considers-appeal-after-court-sides-with-regulator-on-record-privacy-fine, posećeno: 29. 3. 2025.

[90] https://www.edpb.europa.eu/system/files/2023-09/final_decision_tiktok_in-21-9-1_-_redacted_8_september_2023.pdf, 30. 3. 2025.

[91] Data Protection Commission, Irish Data Protection Commission fines LinkedIn Ireland €310 million, 2024, https://dataprotection.ie/en/news-media/press-releases/irish-data-protection-commission-fines-linkedin-ireland-eu310-million, posećeno: 30. 3. 2025.

u iznosu od 60 miliona evra[92], a kompanija *British Airways* 2020. godine sa 20 miliona britanskih funti[93]. Zanimljivo je da je većina ovih i sličnih odluka doneta u Irskoj.

V Zaključak

Slučajevi kompromitacije podataka o ličnosti i povreda GDPR-a u praksi nisu retkost, a sa sobom povlače ozbiljne pravne i finansijske posledice. Međutim, ovi slučajevi predstavljaju samo „vrh ledenog brega", uzimajući u obzir činjenicu da analizirani slučajevi oni o kojima je *javnost obaveštena*.

Uporednopravna analiza pokazuje da, u odnosu na Srbiju, druge države daleko više pažnje posvećuju regulisanju ove materije, a vodeće ekonomije u svetu uveliko ističu značaj korporativnog upravljanja za zaštitu podataka o ličnosti. Uzimajući u obzir visoke kazne u iznosima više milijardi evra, krivičnopravne posledice zloupotrebe podataka o ličnosti, reputacione gubitke i trajni gubitak poverenja, svrsishodno bi bilo ugledati se na stranu literaturu i izvore i prepoznati sajber bezbednosne rizike kao realne rizike poslovanja društva, koji mogu imati ozbiljne posledice i biti izuzetno finansijski iscrpljujuće za kompaniju.

Domaća pravna teorija na neki način zanemaruje važnost ispitivanja odnosa materije korporativnog upravljanja i sajber bezbednosti, a s tim u vezi i značaj zaštite podataka o ličnosti u okviru korporativnog upravljanja. Isto tako, kompanije koje posluju na domaćem tržištu pomalo i ignorišu domaće propise i ne ispunjavaju propisane obaveze, a na internom planu ne čine dovoljno da svoju strukturu i poslovanje prilagode novim poslovnim rizicima koji se odnose na zaštitu podataka o ličnosti. Potrebno je uložiti dodatne napore kako bi trenutna zakonska regulativa odgovorila na potrebe i izazove savremenog poslovanja. Za početak, neophodan je veći angažman i interesovanje naučne zajednice za ova pitanja, uz adekvatnu reformu Kodeksa korporativnog upravljanja, kako bi odredbe bile usaglašene sa Zakonom o zaštiti podataka o ličnosti, a takođe se očekuje i proaktivan rad Poverenika za informacije od javnog značaja i zaštitu podataka o ličnosti.

---

[92] Commission Nationale de l'Informatique et des Libertés, Délibération de la formation restreinte n°SAN-2021-024 du 31décembre 2021 concernant la société x, https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000044840532, posećeno: 30. 3. 2025.

[93] ICO fines British Airways £20m for data breach affecting more than 400,000 customers, https://www.gdprregister.eu/news/british-airways-fine/, posećeno: 30. 3. 2025.

Na neki način, može se reći da dobra praksa korporativnog upravljanja, sajber bezbednost i zaštita podataka o ličnosti predstavljaju „tri musketara" savremenog poslovanja kompanija u digitalnom svetu. Neophodno je da ta „tri musketara" funkcionišu u skladu, sa zajedničkim ciljem – da omoguće bezbedno digitalno poslovanje, koje ne podriva inovacije, a istovremeno štiti pravo na privatnost.

Lidija M. Zečević*

Protection of Personal Data within the Framework of Corporate Governance

Summary

The article analyzes the relationship between corporate governance, cybersecurity and personal data protection. Where appropriate, the author refers to domestic sources and relevant legal norms, emphasizing the fact that Serbian law has not yet recognized the necessity of detailed regulation of this matter. Therefore, the article aims to highlight current trends and recent developments in foreign literature and practice that Serbian law could look up to.

In the first part of the paper, the author points out the significance of personal data and the importance of their legal protection. In the second part of the paper, the author analyzes cybersecurity as a new business risk and explains how corporate governance can respond to it and mitigate it. In the third part of the paper, the author analyzes various cases of cybersecurity attacks that led to data breaches in the largest companies on the market, as well as the significant financial and legal consequences that such attacks had on those companies.

The author further concludes that data breaches can be very debilitating for companies and once again underlines the need to examine the (in)adequacy and (un)preparedness of existing legal regulations to respond to the cybersecurity risks and modern business challenges.

Keywords: corporate governance, personal data protection, data breach, cybersecurity, General Data Protection Regulation (GDPR)

* The author is a third year PhD student at the University of Belgrade, Faculty of Law.

Literatura

Andonović S., „Lice za zaštitu podataka o ličnosti u pravnom sistemu Srbije", u: *Zaštita podataka o ličnosti u Srbiji: zbornik radova* (ur. S. Andonović, D. Prlja, A. Diligenski), Institut za uporedno pravo, Beograd 2020, 117–128.

Andonović S., Prlja D., *Osnovi prava zaštite podataka o ličnosti*, Institut za uporedno pravo, Beograd 2020.

Ashraf M., The Role of Peer Events in Corporate Governance: Evidence from Data Breaches, *The Accounting Review* 97(2022)2, 1–24. https://doi.org/10.2308/TAR-2019-1033

Campbell K., Gordon L. A., Loeb M. P., Zhou L., The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market, *Journal of Computer Security* 11(2003)3, 431–448. https://doi.org/10.3233/JCS-2003-11308

Diligenski A., Prlja D., Cerović D., *Pravo zaštite podataka GDPR*, Institut za uporedno pravo, Beograd 2018.

Gatzlaff K. M., McCullough K. A., The Effect of Data Breaches on Shareholder Wealth, *Risk Management and Insurance Review* 13(2010)1, 61–83. https://doi.org/10.1111/j.1540-6296.2010.01178.x

Goel S., Shawky H. A., Estimating the Market Impact of Security Breach Announcements on Firm Values, *Information & Management* 46(2009)7, 404–410. https://doi.org/10.1016/j.im.2009.06.005

Grove H., Clouse M., Schaffner L. G., Cybersecurity Description and Control Criteria to Strengthen Corporate Governance, *Journal of Leadership, Accountability and Ethics* 16(2019)1, 86–96. https://doi.org/10.33423/jlae.v16i1.1366

Guohong, Z., Zhongwei, X., Feng, H., Zhongyi, X., The Audit Committee's IT Expertise and Its Impact on the Disclosure of Cybersecurity Risk, *Research in International Business and Finance* 73(2025). https://doi.org/10.1016/j.ribaf.2024.102542

Hartmann C. C., Carmenate J., Academic Research on the Role of Corporate Governance and IT Expertise in Addressing Cybersecurity Breaches: Implications for Practice, Policy, and Research, *Current Issues in Auditing* 15(2011)2, A9–A23. https://doi.org/10.2308/CIIA-2020-034

Kiesow Cortez E., Dekker M., A Corporate Governance Approach to Cybersecurity Risk Disclosure, *European Journal of Risk Regulation (EJRR)* 13(2022)3, 443–463. https://doi.org/10.1017/err.2022.10

Kusumawardani S., Rosadi S. D., Gultom E., Good Corporate Governance Principles on Internet Intermediary Companies in Protecting the Privacy of Personal Data in Indonesia, *Yustisia Jurnal Hukum* 9(2020)1, 65–82. https://doi.org/10.20961/yustisia.v9i1.39683

Lehuedé H., Corporate Governance and Data Protection in Latin America and the Caribbean, *Production Development Series*, No. 223 (LC/TS.2019/38), Santiago, Economic Commission for Latin America and the Caribbean (ECLAC), 2019.

Lending C., Minnick K., Schorno P. J., Corporate Governance, Social Responsibility, and Data Breaches, *The Financial Review* 53(2018)2, 413–455. https://doi.org/10.1111/fire.12160

Marutschke H-P., New Developments in German Corporate Governance Law with Focus on Compliance and Data Protection Issues (GDPR), *Doshisha Law Review* 71(2019)1, 57–90.

Monzelo P., Nunes S., "The Role of the Chief Information Security Officer (CISO) in Organizations", in: *19.ª Conferência da Associação Portuguesa de Sistemas de Informação (CAPSI'2019)*, 2019.

Mumtaz Awan T., Riaz Pitafi Z., "Perspective Chapter: Cybersecurity and Risk Management – New Frontiers in Corporate Governance," in: *Corporate Governance - Evolving Practices and Emerging Challenges* (ed. T. Mumtaz Awan), IntechOpen, London 2024. https://doi.org/10.5772/intechopen.1005153

Pérez Carrillo E. F., Cybersecurity in European Financial Institutions: New Grounds for Corporate Governance Reform, *European Business Law Review* 34(2023)7, 1133–1166. https://doi.org/10.54648/EULR2023052

Prlja D., Gasmi G., „Evropska praksa zaštite pojedinaca od zloupotrebe podataka o ličnosti", u: *Zaštita podataka o ličnosti u Srbiji: zbornik radova* (ur. S. Andonović, D. Prlja, A. Diligenski), Institut za uporedno pravo, Beograd 2020, 129–137.

Prlja S., Pravo na zaštitu ličnih podataka u EU, *Strani pravni život* 62(2018)1, 89–99. https://doi.org/10.5937/spz1801089P

Radović V., O približavanju Kodeksa korporativnog upravljanja zakonskoj regulativi, *Teme* 40(2016)3, 1121–1137.

Singh S., Upreti V., Corporate Governance and Cyber Security, *International Journal of Law Management & Humanities* 4(2021)4, 2808–2821.

Tan W., Guo B., Zhang Q., Cybersecurity Governance and Corporate Market Value: Perspectives from Investor Trust and Supply Chain Trust, *Pacific-Basin Finance Journal* 90(2025). https://doi.org/10.1016/j.pacfin.2024.102646

Tikkinen-Piri C., Rohunena A., Markkula J., EU General Data Protection Regulation: Changes and Implications for Personal Data Collecting Companies, *Computer Law & Security Review* 34(2017)1, 134–153. https://doi.org/10.1016/j.clsr.2017.05.015

Tokhadze A., The Interdisciplinary Analysis of Institutional Role of Data Protection Officer in the System of Corporate Governance, *Journal of Personal Data Protection Law* (2023)1.

Internet izvori

Aguilar L. A., Boards of Directors, Corporate Governance and Cyber-Risks: Sharpening the Focus, Cyber Risks and the Boardroom Conference, New York Stock Exchange 2014, https://www.sec.gov/newsroom/speeches-statements/2014-spch061014laa, posećeno: 24. 3. 2025.

Claburn T., Dell customer order database of '49M records' stolen, now up for sale on dark web, 2019, https://www.theregister.com/2024/05/09/dell_data_stolen/, posećeno: 28. 3. 2025.

Conmy S., A cyber security guide for board members, https://www.thecorporategovernanceinstitute.com/insights/guides/cyber-security-guide-board-members/?srsltid=AfmBOorV3WxQusIP5HDr3lSBy7K5d2S_DzMuHdT4_-Sna4_WQ0Sgde86, posećeno: 26. 3. 2025.

Cox O., Kanji H., Building Effective Cybersecurity Governance, 2022, https://corpgov.law.harvard.edu/2022/11/10/building-effective-cybersecurity-governance/, posećeno: 30. 3. 2025.

Data Privacy Manager, 20 biggest GDPR fines so far, 2025, https://dataprivacymanager.net/5-biggest-gdpr-fines-so-far-2020/, posećeno: 29. 3. 2025.

Data Protection Commission, Irish Data Protection Commission fines LinkedIn Ireland €310 million, 2024, https://dataprotection.ie/en/news-media/press-releases/irish-data-protection-commission-fines-linkedin-ireland-eu310-million, posećeno: 30. 3. 2025.

Data Protection Commission, Irish Data Protection Commission fines Meta €251 Million, 2024, https://www.dataprotection.ie/en/news-media/press-releases/irish-data-protection-commission-fines-meta-eu251-million, posećeno: 28. 3. 2025.

DPO Associates, The DPO and the CISO: what is the difference between the two positions?, https://dpoassociates.eu/en/the-dpo-and-the-ciso-what-is-the-difference-between-the-two-positions/, posećeno: 24. 3. 2025.

European Data Protection Board, 1.2 billion euro fine for Facebook as a result of EDPB binding decision, 2023, https://www.edpb.europa.eu/news/news/2023/12-billion-euro-fine-facebook-result-edpb-binding-decision_en, posećeno: 28. 3. 2025.

FTC, Equifax to Pay $575 Million as Part of Settlement with FTC, CFPB, and States Related to 2017 Data Breach, 2019, https://www.ftc.gov/news-events/news/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related-2017-data-breach, posećeno: 27. 3. 2025.

George B., Lyon C., Marcogliese P., Data in the Driver's Seat: What Boards Need to Know about Data Governance, 2024, https://corpgov.law.harvard.edu/2024/04/30/data-in-the-drivers-seat-what-boards-need-to-know-about-data-governance/, posećeno: 26. 3. 2025.

https://www.enforcementtracker.com/, 28. 3. 2025.

https://www.equifaxbreachsettlement.com/, 27. 03. 2025.

ICO fines British Airways £20m for data breach affecting more than 400,000 customers, https://www.gdprregister.eu/news/british-airways-fine/, posećeno: 30. 3. 2025.

Klemash S. W., Smith J. C., Seets C., What Companies are Disclosing About Cybersecurity Risk and Oversight, 2020, https://corpgov.law.harvard.edu/2020/08/25/what-companies-are-disclosing-about-cybersecurity-risk-and-oversight/, posećeno: 24. 3. 2025.

Kroet C., Amazon considers appeal after court sides with regulator on record privacy fine, 2025, https://www.euronews.com/next/2025/03/20/amazon-considers-appeal-after-court-sides-with-regulator-on-record-privacy-fine, posećeno: 29. 3. 2025.

Machilsen K., Haedens E., Why cybersecurity should be a board priority, https://www.ey.com/en_be/insights/cybersecurity/why-cybersecurity-should-be-a-board-priority#:~:text=Therefore%2C%20boards%20must%20prioritize%20cybersecurity,and%20training%20as%20key%20components, posećeno: 24. 3. 2025.

Matić G., Osnove obrade i zaštite podataka – priručnik, https://nsa.gov.rs/extfile/sr/1424/Osnove_obrade_i_zastite_podataka-prirucnik.pdf, posećeno: 29. 3. 2025.

O'Brien S. A., Uber to pay record $148 million over 2016 data breach, 2018, https://money.cnn.com/2018/09/26/technology/uber-settlement-data-breach/index.html?section=money_technology, posećeno: 29. 3. 2025.

Ritzer C., Cyber risk and directors' liabilities: an international perspective, 2016, https://www.nortonrosefulbright.com/en/knowledge/publications/b0dae4a0/cyber-risk-and-directors-liabilitiesan-international-perspective, posećeno: 26. 5. 2025.

SEC, Altaba, Formerly Known as Yahoo!, Charged With Failing to Disclose Massive Cybersecurity Breach; Agrees To Pay $35 Million, 2018, https://www.sec.gov/newsroom/press-releases/2018-71, posećeno: 24. 3. 2025.

SEC, Facebook to Pay $100 Million for Misleading Investors About the Risks It Faced From Misuse of User Data, 2019, https://www.sec.gov/newsroom/press-releases/2019-140, posećeno: 24. 3. 2025.

Share fondacija, Procena rizika od sajber prednji, 2023, https://sharefoundation.info/procena-rizika-od-sajber-pretnji/, posećeno: 29. 3. 2025.

Slijepčević Lj., Privatnost i zaštita podataka o ličnosti kroz domaće i međunarodno pravo s osvrtom na korisnike Fejsbuka i interneta sa krivičnopravnog aspekta, https://pars.rs/public/Dokumenti/Publikacije/1508/Privatnost-i-zastita-podataka-o-licnosti-kroz-domace-i-medjuanrodno-pravo.pdf, posećeno: 30. 3. 2025.

Šta je kibernetička bezbednost?, https://support.microsoft.com/sr-latn-rs/topic/%C5%A1ta-je-sajber-bezbednost-8b6efd59-41ff-4743-87c8-0850a352a390, posećeno: 29. 3. 2025.

Tan A., Emerging stronger together with co-ops – strengthening personal data protection and corporate governance, https://www.mccy.gov.sg/about-us/news-and-resources/speeches/2021/jul/emerging-stronger-together-with-co-ops, posećeno: 24. 3. 2025.

Tester P., Cybersecurity & Data Protection—Key Differences & Benefits, https://datadome.co/learning-center/cybersecurity-and-data-protection/, posećeno: 26. 3. 2025.

U.S. Attorney's Office, Northern District of Georgia, Former Equifax employee sentenced for insider trading, 2019, https://www.justice.gov/usao-ndga/pr/former-equifax-employee-sentenced-insider-trading, posećeno: 27. 3. 2025.

Wanja M. E., Governance in the data age:the application of corproate governance to ensure consumer data protection in Kenya, master thesis, University of Nairobi, 2019, https://erepository.uonbi.ac.ke/bitstream/handle/11295/108799/Mugo_Governance%20in%20the%20Data%20Age-%20the%20Application%20of%20Corporate%20Governance%20to%20Ensure%20Consumer%20Data%20Protection%20in%20Kenya.pdf?sequence=1&isAllowed=y, posećeno: 19. 3. 2025.

Žunić Marić T., Đukanović J., Data Protection Officer vs Country Representative for Serbia, https://zuniclaw.com/en/data-protection-officer-serbia/, posećeno: 30. 3. 2025.

Pravni izvori

Evropska konvencija za zaštitu ljudskih prava i osnovnih sloboda (1950).

Kodeks korporativnog upravljanja, *Službeni glasnik RS*, br. 1/2006.

Kodeks korporativnog upravljanja, *Sl. glasnik RS*, br. 99/2012.

Opšta uredba o zaštiti podataka EU - Regulation 2016/679 of the European Parliament and of the Council on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of such Data, and Repealing Directive 95&46EC (General Data Protection Regulation) od 27. 4. 2016

The Guidebook for Corporate Privacy Governance in the Digital Transformation (DX) Era Ver 1.3, Ministry of Internal Affairs and Communications, Ministry of Economy, Trade and Industry of Japan, 2023, https://www.meti.go.jp/policy/it_policy/privacy/guidebook_ver1.3_english.pdf, posećeno: 21. 3. 2025.

Zakon o zaštiti podataka o ličnosti, *Sl. glasnik RS*, br.87/2018.

Ustav Republike Srbije, *Sl. glasnik RS*, br. 98/2006 i 115/2021.

Univerzalna deklaracija Ujedinjenih nacija o ljudskim pravima (1948).

Sudske i druge odluke

https://www.edpb.europa.eu/system/files/2023-09/final_decision_tiktok_in-21-9-1_-_redacted_8_september_2023.pdf, posećeno: 30. 3. 2025.

Commission Nationale de l'Informatique et des Libertés, Délibération de la formation restreinte n°SAN-2021-024 du 31décembre 2021 concernant la société x, https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000044840532, posećeno: 30. 3. 2025.