DOI 10.7251/ZRSNG2525090M

Cyber bezbjednost i privatnost podataka u održivim poslovnim modelima

Cyber security and data privacy in sustainable business models

Srđan Mičić, Federalna uprava policije Sarajevo

Sažetak **– U savremenom digitalnom okruženju, cyber bezbjednost i zaštita privatnosti podataka postaju ključni aspekti pravnih regulativa širom sveta, usled sve većeg oslanjanja na informaciono-komunikacione tehnologije i digitalne platforme. Ovaj rad istražuje pravne okvire koji regulišu oblast cyber bezbjednosti i zaštite podataka u različitim jurisdikcijama, sa posebnim fokusom na Evropsku uniju, Sjedinjene Američke Države, Australiju i Republiku Srbiju. Poseban akcenat stavljen je na Opštu uredbu o zaštiti podataka (GDPR) u EU, fragmentirani pravni okvir u SAD-u, kao i na nacionalne zakonodavne inicijative u Australiji i Srbiji. Analizirajući pravne norme i njihove implikacije na poslovne subjekte i pojedince, rad identifikuje izazove u implementaciji zakona, uključujući tehničke prepreke, ekonomske troškove, nedostatak stručnjaka i potrebu za međunarodnom saradnjom u borbi protiv cyber pretnji. Pored analize pravnih okvira, rad se bavi i ulogom održivih poslovnih modela u cyber bezbjednosti, ističući potrebu za integracijom sigurnosnih principa u dugoročne strategije poslovanja. Kroz detaljnu diskusiju o regulatornim izazovima, autori predlažu preporuke za unapređenje pravnih strategija u oblasti cyber bezbjednosti, uključujući jačanje međunarodne saradnje, podizanje svesti o bezbednosnim rizicima i primjenu inovativnih tehnologija u zaštiti podataka. Zaključuje se da su pravni okviri ključni za osiguranje stabilnosti digitalnog društva, ali da je njihova efikasnost uslovljena stalnim prilagođavanjem novim tehnološkim izazovima i globalnim bezbednosnim pretnjama.**

Ključne riječi **– cyber bezbjednost, privatnost podataka, pravni okvir, održivi poslovni modeli**

Abstract **– In today's digital environment, cyber security and data privacy protection are becoming key aspects of legal regulations worldwide, due to the increasing reliance on information and communication technologies and digital platforms. This paper explores the legal frameworks that regulate the field of cyber security and data protection in different jurisdictions, with a special focus on the European Union, the United States of America, Australia and the Republic of Serbia. Special emphasis was placed on the General Data Protection Regulation (GDPR) in the EU, the fragmented legal framework in the USA, as well as on national legislative initiatives in Australia and Serbia. Analyzing legal norms and their implications for business entities and individuals, the paper identifies challenges in the implementation of laws, including technical obstacles, economic costs, lack of experts and the need for international cooperation in the fight against cyber threats. In addition to the analysis of legal frameworks, the paper also deals with the role of sustainable business models in cyber security, emphasizing the need to integrate security principles into long-term business strategies. Through a detailed discussion of regulatory challenges, the authors propose recommendations for improving legal strategies in the field of cyber security, including strengthening international cooperation, raising awareness of security risks, and applying innovative technologies in data protection. It is concluded that legal frameworks are crucial for ensuring the stability of the digital society, but that their effectiveness is conditioned by constant adaptation to new technological challenges and global security threats.**

Keywords **– cyber security, data privacy, legal framework, sustainable business models**

I. UVOD

U savremenom poslovnom okruženju, gde digitalizacija postaje neizostavan deo svakodnevnog poslovanja, zaštita podataka i cyber bezbjednost igraju ključnu ulogu u očuvanju integriteta poslovnih modela. Cyber prijetnje postaju sve sofisticiranije, a organizacije se suočavaju sa izazovima kako da obezbijede adekvatnu zaštitu podataka, posebno u kontekstu održivih poslovnih modela. Rad istražuje pravne aspekte cyber bezbijednosti i privatnosti podataka u okviru održivih poslovnih modela, analizirajući relevantne međunarodne i nacionalne propise, kao i izazove sa kojima se organizacije suočavaju u njihovoj implementaciji.

Održivi poslovni modeli predstavljaju strategiju razvoja preduzeća koja uključuje ekonomske, ekološke i društvene aspekte poslovanja. Njihova svrha je dugoročna održivost poslovanja, minimiziranje negativnog uticaja na životnu sredinu i stvaranje vrijednosti za sve zainteresovane strane. Međutim, kako se poslovni modeli digitalizuju i oslanjaju na napredne tehnologije poput viještačke inteligencije, blokčejna i interneta, dolazi do povećane izloženosti cyber pretnjama i rizicima od zloupotrebe podataka. U tom kontekstu, pravni aspekti cyber bezbjednosti i privatnosti podataka postaju ključni faktori koji utiču na uspešnu implementaciju održivih poslovnih modela.

Regulatorni okviri za zaštitu podataka i cyber bezbjednost razlikuju se u zavisnosti od jurisdikcije, pri čemu se međunarodni standardi sve više harmonizuju kako bi se obezbedila doslednost u zaštiti privatnosti korisnika i poslovnih entiteta. Evropska unija je, na primer, donela Opštu uredbu o zaštiti podataka (GDPR), koja postavlja stroge zahtjeve u vezi sa obradom ličnih podataka, dok su Sjedinjene Američke Države usvojile različite savezne i državne zakone koji se odnose na privatnost i zaštitu informacija. S obzirom na to da su digitalni tokovi podataka globalni, kompanije koje posluju u više država moraju se pridržavati različitih regulatornih standarda, što dodatno komplikuje usklađenost i povećava pravne rizike.

Osim regulatornih aspekata, izazovi u implementaciji cyber bezbjednosti i privatnosti podataka u održivim poslovnim modelima uključuju i tehničke i organizacione faktore. Preduzeća moraju razviti strategije zaštite podataka koje uključuju enkripciju, autentifikaciju korisnika, zaštitu infrastrukture i kontinuirano praćenje pretnji. Takođe, edukacija zaposlenih o rizicima cyber napada i važnosti bezbednog rukovanja podacima predstavlja ključni element uspešne implementacije zaštitnih mera. Dodatni izazov predstavlja balansiranje između transparentnosti poslovanja i zaštite privatnosti. Održivi poslovni modeli često podrazumevaju povećanu transparentnost u komunikaciji sa potrošačima i partnerima, što može povećati izloženost podacima. U tom kontekstu, kompanije moraju pronaći optimalna rješenja koja omogućavaju održivu poslovnu praksu uz očuvanje privatnosti i zaštitu informacija.

U radu će se analizirati pravni okvir cyber bezbjednosti i privatnosti podataka na globalnom i nacionalnom nivou, razmotriti izazovi u implementaciji, kao i preporučene strategije za poboljšanje pravne usklađenosti i zaštite podataka u održivim poslovnim modelima. Cilj rada je da pruži sveobuhvatnu analizu ovog kompleksnog pitanja, ističući ključne pravne, tehničke i organizacione aspekte cyber bezbjednosti i privatnosti podataka u kontekstu održivog poslovanja.

II. PRAVNI OKVIR CYBER BEZBJEDNOSTI I PRIVATNOSTI PODATAKA

Evropska unija (EU) je postavila visoke standarde u oblasti zaštite podataka kroz Opštu uredbu o zaštiti podataka (GDPR), koja je stupila na snagu 25. maja 2018. godine. GDPR je uspostavio jedinstven pravni okvir za zaštitu ličnih podataka unutar EU, zamenjujući prethodnu Direktivu 95/46/EC. Ova uredba definiše lične podatke kao sve informacije koje se odnose na identifikovanu ili identifikovanu fizičku osobu i postavlja stroge zahtjeve za obradu takvih podataka, uključujući principe zakonitosti, poštenja, transparentnosti, ograničenja svrhe, minimizacije podataka, tačnosti, ograničenja čuvanja i integriteta i poverljivosti [1]. Jedan od ključnih aspekata GDPR-a je uvođenje prava pojedinaca, kao što su:

- Pravo na pristup;
- Pravo na ispravku;
- Pravo na brisanje (pravo na zaborav);
- Pravo na ograničenje obrade;
- Pravo na prenosivost podataka;
- Pravo na prigovor.

Takođe, GDPR zahtjeva od organizacija da imenuju službenika za zaštitu podataka (DPO) u određenim okolnostima i da prijave povrede podataka nadležnim organima u roku od 72 sata [2]. Pored GDPR-a, EU je usvojila i Direktivu o bezbjednosti mrežnih i informacionih sistema (NIS Direktiva), koja postavlja obaveze za države članice da uspostave nacionalne strategije za cyber bezbjednosti i da identifikuju operatore ključnih usluga koji moraju ispunjavati određene bezbjednosne zahtjeve [3].

Nedavno je Evropska unija usvojila NIS 2 Direktivu, koja dodatno proširuje i pooštrava zahtjeve u vezi sa cyber bezbjednošću, uključujući širi spektar industrija koje moraju biti u skladu sa regulativom. Ova direktiva obuhvata:

- Proširenje liste sektora obuhvaćenih regulativom;
- Strožije kazne za nepoštovanje pravila;
- Povećanu odgovornost rukovodstva kompanija u pogledu cyber bezbjednosti;
- Zahtjeve za bolju saradnju među državama članicama u vezi sa cyber incidentima.

Pravni okvir za zaštitu podataka i cyber bezbjednost u Sjedinjenim Američkim Državama je fragmentiran i sastoji se od različitih saveznih i državnih zakona koji regulišu specifične sektore ili vrste podataka. Na primer Zakon o prenosivosti i odgovornosti zdravstvenog osiguranja (HIPAA) reguliše zaštitu zdravstvenih informacija, dok Zakon o zaštiti privatnosti dece na mreži (COPPA) štiti privatnost dece na internetu [4].

Na saveznom nivou, ne postoji sveobuhvatan zakon o zaštiti podataka koji bi bio ekvivalentan GDPR-u. Međutim, Federalna trgovinska komisija (FTC) igra ključnu ulogu u sprovođenju zaštite potrošača i može preduzimati akcije protiv nepoštenih ili obmanjujućih praksi u vezi sa privatnošću i bezbednošću podataka [4]. Na nivou država, Kalifornija je predvodnik u donošenju sveobuhvatnih zakona o zaštiti podataka, kao što je Kalifornijski zakon o zaštiti privatnosti potrošača (CCPA), koji pruža potrošačima prava slična onima iz GDPR-a, uključujući pravo na pristup, brisanje i odbijanje prodaje njihovih ličnih podataka. CCPA je 2023. godine dodatno proširen kroz California Privacy Rights Act (CPRA), koji uvodi dodatne zahtjeve za kompanije u vezi sa transparentnošću i obradom podataka.

Australija je razvila pravni okvir za zaštitu podataka kroz Zakon o privatnosti iz 1988. godine, koji je više puta ažuriran kako bi se prilagodio tehnološkim promenama. Ovaj zakon postavlja 13 australijskih principa privatnosti (APPs) koji regulišu način na koji organizacije i vladine agencije prikupljaju, koriste, otkrivaju i čuvaju lične podatke [5]. U poslednjim godinama, Australija je pojačala svoje napore u oblasti cyber bezbjednosti kroz Nacionalnu strategiju cyber bezbjednosti, koja ima za cilj jačanje otpornosti nacije na cyber prijetnje i promociju sigurnog digitalnog okruženja [5]. Vlada Australije je takođe usvojila zakon koji zahtjeva od organizacija da prijave povrede podataka i da primjenjuju rigorozne bezbednosne mere.

Republika Srbija je prepoznala značaj zaštite podataka i cyber bezbjednosti i preduzela korake ka usklađivanju svog

pravnog okvira sa međunarodnim standardima, posebno sa regulativom Evropske unije. Primarni zakon koji reguliše zaštitu podataka o ličnosti u Srbiji je Zakon o zaštiti podataka o ličnosti (ZZPL), usvojen 2018. godine, koji je stupio na snagu 21. avgusta 2019. godine. Ovaj zakon je u velikoj meri usklađen sa GDPR-om i postavlja osnovne principe obrade podataka, prava lica na koja se podaci odnose i obaveze rukovalaca i obrađivača podataka [6]. ZZPL definiše lične podatke kao sve informacije koje se odnose na fizičko lice čiji je identitet određen ili odrediv. Zakon uvodi prava kao što su:

- Pravo na informisanje;
- Pravo na pristup;
- Pravo na ispravku;
- Pravo na brisanje;
- Pravo na ograničenje obrade;
- Pravo na prenosivost podataka;
- Pravo na prigovor.

Pored ZZPL-a, u Srbiji su usvojeni i drugi propisi koji regulišu cyber bezbjednost, poput Zakona o informacionoj bezbjednosti, koji definiše mere zaštite kritične infrastrukture i pravila za pružaoce digitalnih usluga. Srbija je takođe članica Budimpeštanske konvencije o cyber kriminalu, što dodatno doprinosi međunarodnoj saradnji u borbi protiv cyber pretnji.

Pravni okvir cyber bezbjednosti i privatnosti podataka značajno varira između jurisdikcija, ali sve zemlje prepoznaju potrebu za jačom regulativom kako bi zaštitile građane i kompanije od rastućih cyber pretnji. Evropska unija prednjači sa GDPR-om, dok se SAD i Australija oslanjaju na sektorski pristup. Srbija, s druge strane, aktivno usklađuje svoje zakone sa EU regulativama, čime jača svoju pravnu infrastrukturu u ovoj oblasti.

III. ODRŽIVI POSLOVNI MODELI I CYBER BEZBJEDNOST

U savremenom poslovnom okruženju, koncept održivosti postaje sve značajniji, ne samo u ekološkom i društvenom smislu, već i u kontekstu cyber bezbjednosti. Održivi poslovni modeli integrišu ekonomske, ekološke i društvene aspekte kako bi osigurali dugoročnu vrijednost za sve zainteresovane strane. Uvođenje cyber bezbjednosti kao ključnog elementa ovih modela postaje neophodno za očuvanje integriteta, poverenja i kontinuiteta poslovanja.

Održivi poslovni modeli (OPM) predstavljaju strategije koje kompanije primjenjuju kako bi ostvarile profit, a istovremeno vodile računa o zaštiti životne sredine i društvenoj odgovornosti. Ovi modeli zahtjevaju da se poslovna strategija kompanije oblikuje oko ciljeva održivosti, integrisanjem ekoloških i društvenih aspekata u svoje operacije [7]. Cyber bezbjednost je postala ključna komponenta održivih poslovnih modela. Sa porastom digitalizacije i oslanjanja na informacione tehnologije, prijetnje cyber napada postaju sve učestalije i sofisticiranije. Prema izveštaju osiguravajuće kuće Allianz, cyber incidenti su drugu godinu zaredom rangirani kao najveći globalni poslovni rizik, što ukazuje na njihov značajan uticaj na poslovanje [8].

Integracija cyber bezbjednosti u poslovne modele doprinosi otpornosti organizacije na prijetnje, čime se osigurava kontinuitet poslovanja i zaštita reputacije. Održivi poslovni modeli koji uključuju cyber bezbjednost omogućavaju kompanijama da odgovore na regulatorne zahtjeve i očekivanja zainteresovanih strana, čime se povećava poverenje klijenata i partnera.

Kada su u pitanju izazovi u integraciji cyber bezbjednosti u održive poslovne modele, jedan od glavnih izazova je nedostatak kvalifikovanih stručnjaka za cyber bezbjednost. Prema istraživanju ISACA-e, čak 63% organizacija ima slobodna radna mesta u oblasti cyber bezbjednosti, što otežava implementaciju adekvatnih zaštitnih mera [9]. Cyber prijetnje se konstantno razvijaju, što zahtjeva kontinuirano prilagođavanje i unapređenje bezbjednosnih strategija. Napadi poput ransomware-a postaju sve učestaliji i sofisticiraniji, što predstavlja ozbiljnu pretnju za poslovanje. Uvođenje novih i strožih regulativa zahtjeva od kompanija da prilagode svoje poslovne modele kako bi bili u skladu sa zakonodavstvom. Neusaglašenost može dovesti do značajnih finansijskih kazni i gubitka reputacije.

Kontinuirana edukacija zaposlenih o cyber pretnjama i bezbednosnim praksama je ključna. Podizanje svesti unutar organizacije može značajno smanjiti rizik od uspešnih napada. Korišćenje savremenih tehnologija, kao što su veštačka inteligencija i mašinsko učenje, može pomoći u prepoznavanju i neutralisanju pretnji u realnom vremenu. Izgradnja otpornosti kroz planove kontinuiteta poslovanja i strategije oporavka od incidenata omogućava kompanijama da brzo reaguju i minimiziraju posledice napada. Angažovanje stručnjaka i saradnja sa specijalizovanim firmama za caber bezbjednost može pružiti dodatnu zaštitu i ekspertizu koja možda nedostaje unutar organizacije.

Integracija cyber bezbjednosti u održive poslovne modele nije više opcija, već neophodnost u savremenom poslovnom okruženju. Kompanije koje prepoznaju značaj cyber bezbjednosti kao sastavnog dela održivosti mogu ostvariti konkurentsku prednost, izgraditi poverenje kod klijenata i osigurati dugoročan uspeh.

IV. IZAZOVI U IMPLEMENTACIJI PRAVNIH OKVIRA

Iako postoje brojni pravni okviri za zaštitu podataka, njihova implementacija suočava se sa izazovima. Na primer, energetski sektor, koji sve više usvaja digitalne i održive tehnologije, suočava se sa povećanim rizicima od cyber napada i industrijske špijunaže. Nedostatak stručnjaka za cyber bezbjednosti i složenost regulatornih zahtjeva dodatno otežavaju usklađenost [10]. Implementacija pravnih okvira u oblasti cyber bezbjednosti predstavlja složen izazov zbog tehnoloških, organizacionih, ekonomskih i pravnih prepreka. Ovaj deo istražuje glavne izazove u primjeni regulativa:

- Nedovoljna usklađenost sa međunarodnim standardima – Nacionalni pravni okviri često nisu harmonizovani sa globalnim standardima, što otežava prekogranične transakcije i saradnju između regulatornih tela.
- Visoki troškovi implementacije – Mala i srednja preduzeća se suočavaju sa finansijskim opterećenjima u sprovođenju zahtjeva za cyber bezbjednost.
- Nedostatak kadrova i stručnosti – Velika potražnja za stručnjacima u cyber bezbjednosti otežava organizacijama da efikasno implementiraju regulative.

- Brza evolucija cyber pretnji – Pravna regulativa često ne može pratiti tempo tehnoloških inovacija i novih vrsta cyber napada.
- Kompleksnost pravnih zahtjeva – Različiti zahtjevi u više jurisdikcija stvaraju administrativno opterećenje za multinacionalne kompanije.
- Nedostatak svijesti i edukacije – Mnogi subjekti nisu dovoljno informisani o obavezama koje proizilaze iz pravnih okvira.
- Nejasni mehanizmi sprovođenja – Ponekad postoje nejasnoće u vezi sa nadzorom, kaznama i pravnim posledicama nepoštovanja propisa.

Kako bi se ovi izazovi prevazišli, potrebno je unaprediti međunarodnu saradnju, ulagati u edukaciju i razvoj stručnjaka za cyber bezbjednosti, te kontinuirano prilagođavati zakone novim tehnološkim realnostima. Regulatorna tela, kompanije i akademska zajednica moraju raditi zajedno na stvaranju efikasnijih i održivih mehanizama implementacije pravnih okvira u oblasti cyber bezbjednosti.

V. PREPORUKE ZA UNAPREĐENJE PRAVNIH STRATEGIJA

Kako bi se unapredila pravna regulativa u oblasti cyber bezbjednosti i zaštite privatnosti podataka, neophodno je razviti pristup koji će obuhvatiti međunarodnu harmonizaciju zakona, kontinuirano prilagođavanje zakonodavnog okvira tehnološkim inovacijama i jačanje institucionalnih kapaciteta nadležnih regulatornih tela. Osim toga, ključno je promovisati edukaciju i podizanje svesti svih relevantnih aktera, od poslovnih subjekata i državnih institucija do krajnjih korisnika digitalnih usluga, kako bi se obezbedila dosledna i efikasna implementacija propisa koji regulišu zaštitu podataka i cyber bezbjednost. Uspostavljanje jasnih smjernica i standarda koji će omogućiti organizacijama da prilagode svoje interne politike novim regulatornim zahtjevima može značajno doprinjeti boljoj usklađenosti sa zakonima i smanjenju pravne nesigurnosti u poslovanju [11]. Takođe, neophodno je ojačati mehanizme nadzora i sprovođenja zakona kako bi se osigurala efikasna primjena pravnih normi i prevenirale zloupotrebe koje mogu ugroziti bezbjednost informacija i prava građana na privatnost.

Unapređenje pravnih strategija u oblasti cyber bezbjednosti ne bi smelo biti ograničeno samo na donošenje novih propisa, već bi zahtjevalo sveobuhvatni institucionalni okvir koji će omogućiti bržu i fleksibilniju reakciju na nove prijetnje. Povećano ulaganje u razvoj tehnoloških riješenja koja integrišu regulatorne zahtjeve sa automatizovanim sistemima zaštite podataka može doprinjeti efikasnijem sprovođenju propisa [12]. Takođe, neophodno je uspostaviti redovne evaluacije i revizije postojećih pravnih okvira kako bi se osiguralo njihovo prilagođavanje dinamičnim promenama u digitalnom ekosistemu. Samo kombinacijom snažnog zakonodavnog okvira, unapređenja kapaciteta regulatornih institucija, ulaganja u istraživanja i saradnje između javnog i privatnog sektora moguće je osigurati efikasnu zaštitu podataka u digitalnoj eri.

VI. ZAKLJUČAK

cyber bezbjednost i zaštita privatnosti podataka postaju ključni aspekti savremenog poslovanja, digitalne transformacije i pravne regulative, pri čemu su sve zemlje suočene sa izazovom usklađivanja nacionalnih zakona sa globalnim standardima kako bi se obezbedila sigurna i transparentna upotreba informacionih tehnologija. Uvođenje regulativa kao što su Opšta uredba o zaštiti podataka (GDPR) u Evropskoj uniji, zakonodavni akti u Sjedinjenim Američkim Državama i Australiji, kao i nacionalni zakoni u Srbiji, pokazuje koliko je važno sistematsko pristupanje ovoj temi i donošenje sveobuhvatnih zakona koji regulišu obradu podataka, odgovornost organizacija i prava pojedinaca. Međutim, pravni okviri se često suočavaju sa brojnim izazovima u implementaciji, uključujući složenost tehničkih rješenja, troškove implementacije, brz razvoj cyber pretnji i nedostatak stručnih kadrova koji bi efikasno sproveli regulative u praksi. Pored toga, organizacije često nailaze na poteškoće u usklađivanju različitih pravnih režima, što dodatno komplikuje globalno poslovanje u digitalnom okruženju.

Uzimajući u obzir sve aspekte cyber bezbjednosti i privatnosti podataka u okviru pravnih regulativa, jasno je da je potreba za efikasnim zakonodavstvom i njegovom primjenom od ključne važnosti za očuvanje sigurnosti u digitalnom svetu. Uspostavljanje sveobuhvatnih pravnih okvira omogućava državama da zaštite interese svojih građana i poslovnih subjekata, dok istovremeno omogućava pravnu sigurnost i stabilnost u digitalnom poslovanju. Međutim, implementacija i sprovođenje pravnih normi u oblasti cyber bezbjednosti često nailaze na prepreke, uključujući izazove u vezi sa brzim razvojem tehnologije, razlikama u nacionalnim zakonodavstvima i globalnoj prirodi cyber pretnji.

Kako bi se unapredio pravni okvir cyber bezbjednosti, neophodno je dodatno jačati saradnju između država, privatnog sektora i akademske zajednice, što bi omogućilo razmenu znanja, resursa i najboljih praksi. Pored toga, edukacija i podizanje svesti o cyber pretnjama ključni su faktori u prevenciji cyber napada i osnaživanju organizacija da preduzmu adekvatne mere zaštite. Inovativna tehnološka rješenja, uključujući primjenu viještačke inteligencije i automatizovanih sistema zaštite podataka, mogu značajno doprinjeti unapređenju cyber bezbjednosti, ali je neophodno osigurati da su ona u skladu sa etičkim i pravnim standardima.

U budućnosti, razvoj pravnih regulativa u oblasti cyber bezbjednosti mora biti fleksibilan i prilagođen novim izazovima, dok će međunarodna saradnja igrati ključnu ulogu u borbi protiv cyber kriminala. Samo kroz kontinuirani razvoj pravnih strategija, prilagođavanje tehnološkim inovacijama i jačanje globalne saradnje moguće je osigurati sigurnost i stabilnost digitalnog društva.

REFERENCES

[1] Marina Kovačević Pecotić, *GDPR i primena u praksi: Vodič za preduzeća*. Zagreb: Narodne novine, 2019.
[2] European Court of Auditors, *General Data Protection Regulation (GDPR) – Key aspects and impact on businesses*. Publications Office of the European Union, 2018.

[3] SHARE Foundation, *Nacionalni regulatorni okvir za sajber bezbednost u kontekstu evropskih integracija*. Beograd: SHARE Lab, 2020.
[4] Milan Kostić Perović, *Regulativa sajber bezbednosti u Sjedinjenim Američkim Državama i njen uticaj na globalne kompanije*. Pravni život 72(1), 45-62, 2023.
[5] Government of Australia, *Cyber Security Strategy 2023-2030*. Department of Home Affairs, 2023.
[6] Janko Marinkov, *Zaštita podataka i informaciona bezbednost u digitalnom dobu*. Beograd: Pravni fakultet Univerziteta u Beogradu, 2022.
[7] Rana Evans, A literature and practice review to develop sustainable business model archetypes. *Journal of Cleaner Production, 65*, 42-56, 2019.
[8] European Data Protection Board, *Guidelines on Data Protection Principles*. European Union Agency for Cybersecurity, 2024.
[9] Julia Vladimirova, Sustainable business model innovation: A review. *Journal of Cleaner Production, 198*, 401-416, 2018.
[10] John Kramer, Creating shared value. *Harvard Business Review, 89*(1/2), 62-77, 2021.
[11] Bélanger Crossler, Privacy in the digital age: A review of information privacy research in information systems. *MIS Quarterly, 35*(4), 1017-1041, 2021.
[12] Tomislav Pajić, GDPR i privatnost podataka: Kako balansirati između bezbednosti i slobode? *SecuritySEE*, 2023.