

ELEKTRONSKO PLAĆANJE U DIGITALNOJ EKONOMIJI I PRAVNI ASPEKTI ZAŠTITE POTROŠAČA U BOSNI I HERCEGOVINI

Autor: MARKO GAJIĆ, Boris Đukić

e-mail: marko.gajic@student.ef.unibl.org, boris.djukic@student.pf.unibl.org

Mentor: prof. dr Ljubiša Mičić

Ekonomski fakultet Univerziteta u Banjoj Luci

Pravni fakultet Univerziteta u Banjoj Luci

Uvod: Elektronsko plaćanje je brzo rastuća oblast savremenog platnog prometa, zasnovana na tehnologijama poput tokenizacije, višefaktorske autentifikacije i enkripcije, koje obezbjeđuju sigurnost transakcija. Istovremeno, pravna regulativa (EU direktive i domaći zakoni) omogućava zaštitu potrošača od zloupotreba, a u radu iznosimo zaključke o razvoju elektronskog plaćanja na našem tržištu.

Cilj: Cilj ovog rada je da s jedne strane identifikuje ključne sigurnosne tehnologije koje omogućavaju bezbjedno izvršavanje digitalnih transakcija, dok sa druge strane sagledava pravni okvir i efikasnost važeće regulative.

Materijali i metode: Autori su prilikom izrade rada koristili kombinaciju kvalitativnih i komparativnih metoda istraživanja. Analiza konkretnih platformi obuhvaćena je studijom slučaja (PayPal). Materijali obuhvataju stručnu literaturu iz oblasti poslovne informatike, finansija i prava, te važeće zakonske propise i evropske direktive.

Rezultati: Istraživanje je pokazalo da elektronsko plaćanje nudi značajne prednosti u pogledu brzine i dostupnosti transakcija, ali i da nosi rizike vezane za sigurnost podataka i moguće zloupotrebe. Analiza zakonskog okvira ukazuje na to da PSD2 i GDPR pružaju širok spektar mehanizama za zaštitu potrošača, dok domaći zakoni u regionu često kasne u implementaciji. Sa tehničke strane, savremene platforme primjenjuju napredne sigurnosne mjere poput enkripcije i višefaktorske autentifikacije, što značajno smanjuje rizik od prevara. Analiza platforme PayPal pokazuje da globalni servisi imaju razvijenije mehanizme zaštite i transparentnije politike, dok lokalne banke tek djelimično prate ove standarde.

Zaključak: Elektronsko plaćanje predstavlja temelj digitalne ekonomije, ali njegova održivost zavisi od sinergije između pravne regulative i tehnoloških rješenja. Analiza je pokazala da globalne platforme prednjače u primjeni sigurnosnih tehnologija i transparentnih pravila, dok lokalni sistemi zahtijevaju dodatna ulaganja i usklađivanje sa međunarodnim standardima.

Ključne riječi: elektronsko plaćanje, digitalna ekonomija, zaštita potrošača, poslovna informatika, pravna regulativa.

UVOD

Fuzija informacionih tehnologija i tradicionalne ekonomije, pod nazivom digitalna ekonomija, omogućila je transformaciju tradicionalnih ekonomskih aktivnosti u automatizovane procese koji se zasnivaju na digitalnim tehnologijama. Digitalna ekonomija podrazumijeva aktivnosti poput e-trgovine, digitalnog marketinga, implementacije interneta stvari (IoT), računarstva u oblaku (*Cloud computing*) te je označena kao jedan od pokretača inovacija, povećanja produktivnosti i globalnog ekonomskog rasta (Xia, 2024).

Razvoj digitalne ekonomije, praćen evolucijom i napretkom informacionih tehnologija,

čiji je razvoj ubrzan posljednjih godina, učinio je digitalnu ekonomiju snažnom pokretačkom silom ekonomskog rasta i razvoja koja vodi globalnu ekonomiju ka digitalizaciji.

Digitalna ekonomija ima značajne uticaje na različite ekonomske, društvene i kulturne sfere, uključujući promjene u načinu na koji ljudi rade i međusobno komuniciraju, podstičući fleksibilnije i udaljeno (remote) obavljanje poslova, kao i povećanu globalnu povezanost. Takođe, digitalna ekonomija je uticala na obrazovanje, zdravstvo, zabavu i druge sektore.

Komponenta digitalne ekonomije na koju će se ovaj rad fokusirati jeste elektronsko plaćanje, kao i zaštita potrošača pomoću sigurnosnih tehnologija i pravnih instrumenata. Razvoj tehnologije uslovio je virtuelizaciju procesa plaćanja uvođenjem elektronskih sistema plaćanja koji su razlikuju od tradicionalnih sistema po digitalizovanim sredstvima plaćanja i automatizovanoj obradi transakcija. U sistemima elektronskog plaćanja mogu se izdvojiti tri ključne uloge: kupac, prodavac i procesor plaćanja. Kupac inicira proces plaćanja i bira metod plaćanja (na primjer, PayPal, Visa kartica, plaćanje pouzećem). Prodavac na svom veb-sajtu može omogućiti više metoda plaćanja, od kojih kupac bira koju metodu će koristiti. Procesor plaćanja je posrednik preko kojeg se omogućava prodavcima da u trgovini putem interneta naplaćuju platnim karticama. Jedan od najpoznatijih globalnih procesora plaćanja je PayPal, o kojem će biti više riječi u nastavku rada (Radenković, 2015).

Kao što nalaže IMRAD metodologija, čitaoci ovog rada će na početku biti upoznati sa osnovnim pojmovima i ciljem ovog rada.

METODE I MATERIJALI

Za potrebe ovog rada korišteni su različiti izvori i metodološki pristupi, kako bi se obezbijedila interdisciplinarna analiza elektronskog plaćanja i zaštite potrošača u digitalnoj ekonomiji. Materijal obuhvata stručnu literaturu iz oblasti poslovne informatike, digitalne ekonomije i prava, sa naglaskom na sigurnosne tehnologije u elektronskom plaćanju, pravni okvir zaštite potrošača i aktuelne izazove u praksi. U analizu su uključeni domaći i međunarodni naučni radovi, kao i relevantna zakonska i regulatorna dokumenta.

Poseban značaj u ovom radu ima sekundarno istraživanje (Hassan, 2020), koje je analiziralo veliku bazu objavljenih naučnih i stručnih radova o elektronskom poslovanju. Cilj tog istraživanja bio je da se identifikuju ključni problemi koji koče širu primjenu i razvoj elektronskog poslovanja na globalnom nivou. Rezultati pokazuju da među najveće izazove spadaju: sigurnost i privatnost, jer korisnici često izražavaju bojazan da će njihovi lični i finansijski podaci biti zloupotrijebljeni; nedostatak povjerenja u elektronske servise, posebno kod novih i manjih pružalaca usluga; pravna i regulatorna ograničenja, budući da postoji značajna neusklađenost zakona među državama; zatim tehničke barijere, poput nepouzdatih sistema i složenih procedura; kao i korisničko iskustvo, koje često nije dovoljno jednostavno i transparentno za krajnje potrošače. Ovi nalazi poslužili su kao teorijska osnova za dalje razmatranje teme i okvir za analizu studije slučaja.

Sa pravnog aspekta, u radu su analizirani zakoni Bosne i Hercegovine koji se odnose na zaštitu potrošača, elektronsku trgovinu i platne usluge. Pored domaćih propisa, razmatrane su i relevantne direktive Evropske unije, među kojima posebno mjesto zauzimaju Direktiva o pravima potrošača i Direktiva o platnim uslugama (PSD2), koje postavljaju standarde sigurnosti i transparentnosti u oblasti elektronskih transakcija. Uključivanjem ovih dokumenata omogućeno je poređenje domaćeg zakonodavstva sa evropskim okvirom, kao i identifikacija oblasti u kojima su potrebna dodatna usklađivanja.

Metodološki okvir rada zasnovan je na više pristupa, pri čemu je deskriptivno-analitička metoda korištena za pregled, sistematizaciju i interpretaciju stručne literature i zakonskih propisa, komparativna metoda omogućila je poređenje različitih regulatornih i tehnoloških

rješenja, sa posebnim fokusom na razlike između domaćeg i evropskog zakonodavstva, ali i između globalnih i lokalnih platnih platformi. Studija slučaja primijenjena je kroz analizu platforme **PayPal**, koja je odabrana zbog svoje globalne raširenosti i visokog nivoa povjerenja među korisnicima. Analiza PayPal-a obuhvatila je pregled njegovih sigurnosnih tehnologija (enkripcija podataka, tokenizacija, višefaktorska autentifikacija), procedura zaštite korisnika (refundacije, rješavanje sporova), kao i politike usklađenosti sa pravnim okvirima Evropske unije i drugih jurisdikcija. Na ovaj način PayPal je poslužio kao praktičan primjer kako se u praksi mogu implementirati mehanizmi zaštite potrošača, ali i kao referenca za poređenje sa lokalnim rješenjima.

Kombinovanjem pravnog i informatičkog pristupa obezbijeđen je integrisan okvir istraživanja. Takav pristup omogućava sagledavanje elektronskog plaćanja i zaštite potrošača iz dvije komplementarne perspektive: pravne, koja garantuje institucionalnu sigurnost i povjerenje, i informatičke, koja pruža tehničku osnovu za pouzdanost i sigurnost transakcija. Interdisciplinarna metodologija korištena u ovom radu osigurava ne samo teorijski doprinos već i praktične implikacije za unapređenje elektronskog plaćanja u digitalnoj ekonomiji.

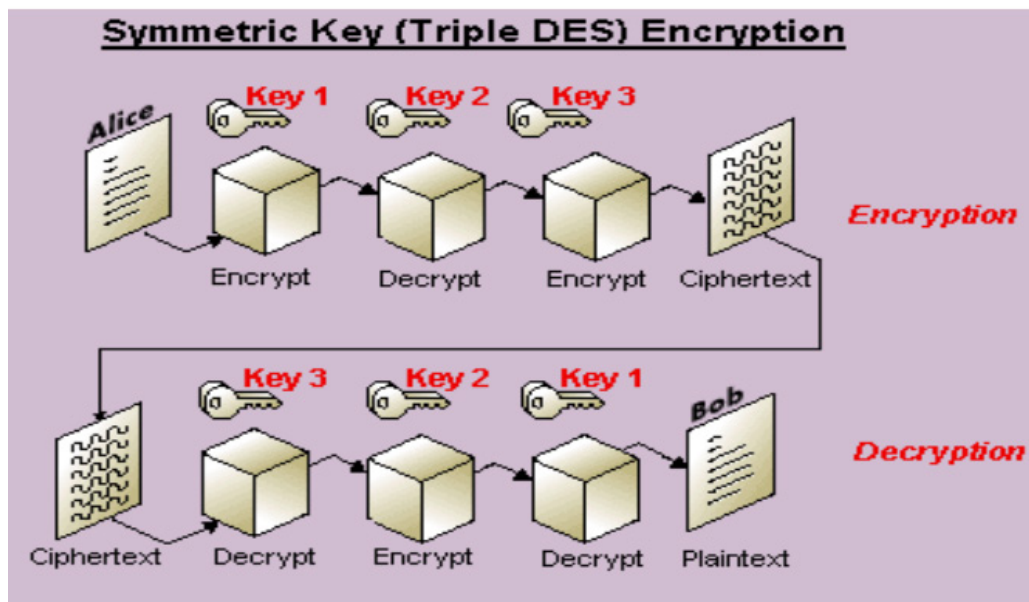
REZULTATI

Analiza pregleda literature o elektronskom poslovanju, koja je obuhvatila više od 130 naučnih i stručnih radova u periodu od 2010. do 2020. godine, pokazala je da su najčešći izazovi vezani za sigurnost, povjerenje korisnika i pravnu regulaciju. Autori posebno naglašavaju da se prepreke razvoju elektronskog poslovanja u najvećoj mjeri odnose na zaštitu ličnih i finansijskih podataka, rizik od zloupotreba identiteta, te nedostatak povjerenja potrošača u pouzdanost digitalnih platformi. Identifikovano je i da su od ključne važnosti tehnički zahtjevi poput: povjerljivosti podataka, integriteta transakcija, autentifikacije korisnika, autorizacije pristupa, neraskidivosti transakcije i dostupnosti sistema. Svi ovi elementi čine temelj sigurnog elektronskog plaćanja i direktno utiču na nivo spremnosti potrošača da koriste digitalne kanale.

Kako bi se prevazišli ovi izazovi i izgradilo povjerenje korisnika, u praksi su razvijeni različiti sigurnosni mehanizmi i tehnologije koje obezbjeđuju zaštitu transakcija u elektronskom plaćanju. U nastavku rada, pažnja će biti posvećena najznačajnijim sigurnosnim tehnologijama.

Osnovu sigurnosti kod elektronskih transakcija predstavlja sigurnosni protokol SET (Secure Electronic Transaction), koji koristi kriptografiju kako bi obezbijedio povjerljivost podataka, garantovao integritet plaćanja i omogućio autentifikaciju identiteta. Secure Electronic Transaction (SET) uključuje tri strane: vlasnika kreditne ili debitne kartice, trgovca i banku kao platni prolaz (payment gateway). Vlasnik kreditne ili debitne kartice dijeli informacije o porudžbini sa trgovcem putem veb-sajta trgovca, ali ne i sa bankom (platnim prolazom). Međutim, vlasnik kreditne ili debitne kartice dijeli informacije o plaćanju sa platnim prolazom (bankom), ali ne i sa trgovcem. U okviru Secure Electronic Transaction (SET) protokola koriste se različiti algoritmi za enkripciju, kao što su DES (Data Encryption Standard) i RSA algoritam. Data Encryption Standard (DES) je algoritam sa ključem dužine 56 bita, koji se koristi za enkripciju onlajn transakcija (Dijesh, 2020).

Ova tehnika enkripcije nije bila dovoljno bezbjedna te se može vrlo lako probiti sa modernim softverima. Sa razvojem tehnologije razvijale su se i tehnike enkripcije, pa je tako nastala višestruka enkripcija. Višestruka enkripcija je tehnika za unapređenje bezbjednosti podataka tako što se proces enkripcije izvodi više puta koristeći isti ili različite tipove enkripcionih ključeva. Višestruka enkripcija povećava složenost zaštite podataka na takav način da uljez ili neovlašćeni korisnik ne može dekriptovati podatke, čak i ako



Slika 1. Proces enkripcije. Izvor: Autor

su mu poznati neki enkripcijski ključevi (Gupta, 2011).

Višefaktorska autentifikacija (MFA) je sigurnosna tehnika koji zahtijeva od korisnika da pruže dva ili više nezavisna akreditiva kako bi potvrdili svoj identitet prije nego što dobiju pristup digitalnim sistemima. Kako sajber prijetnje rastu, a tradicionalne lozinke postaju ranjive, višefaktorska autentifikacija se danas široko koristi u elektronskom bankarstvu, korporativnim sistemima, IoT uređajima i ličnim nalogima, kako bi se obezbijedila jača zaštita od neovlašćenog pristupa.

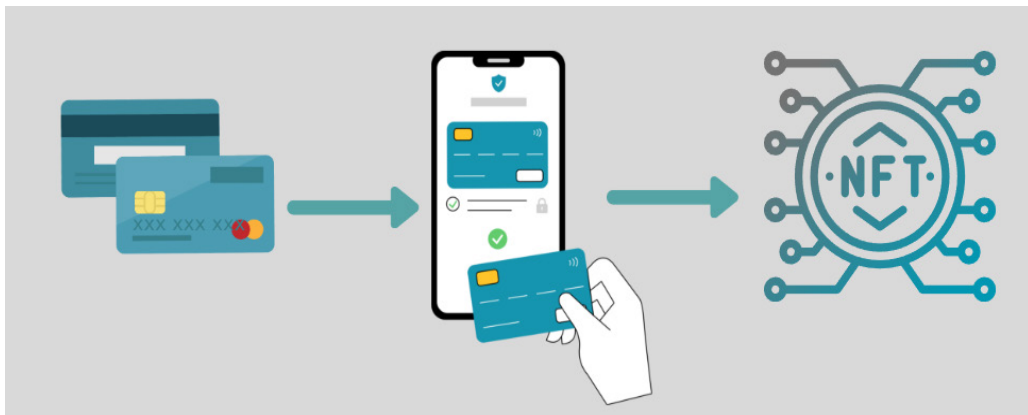


Slika 2. Proces višefaktorske autentifikacije. Izvor: Autor

Prvi faktor obuhvata nešto što korisnik zna, kao što su lozinka, PIN kod ili sigurnosno pitanje. Drugi faktor podrazumijeva mobilni telefon, karticu ili jednokratnu lozinku, odnosno nešto što korisnik posjeduje. Treći faktor višefaktorske autentifikacije su biometrijski podaci poput otiska prsta ili prepoznavanja lica, ono što korisnik jeste (Ometov, 2018).

Tokenizacija plaćanja je proces u kojem se podaci sa platne kartice ne čuvaju kod trgovca, već se zamjenjuju nasumičnim tokenom, nizom znakova iste dužine kao i broj kartice. Originalni podaci se sigurno skladište u posebnom „digitalnom trezoru“ (token vault), dok se za transakciju koristi samo token. Na ovaj način, trgovac nikada nema pristup stvarnim podacima kartice, već vidi samo token koji služi za obradu plaćanja kroz banke i kartične mreže. Kada korisnik sljedeći put kupuje kod istog trgovca, dovoljno je da koristi token, što omogućava brzo plaćanje, dok pravi podaci ostaju zaštićeni. Trgovci

tako zadržavaju povjerenje kupaca, čuvaju reputaciju i ostaju u skladu sa PCI-DSS standardom (Payment Card Industry Data Security Standard). Tokenizacija tako podiže nivo bezbjednosti, jer čak i ako token bude presretnut, on nema vrijednost van svog sistema i ne može otkriti originalne podatke kartice (How Does Payment Tokenization Work?, 2021).



Slika 3. Ilustracija tokenizacije. Izvor: Autor

ZAKONSKA REGULATIVA

Tendencija porasta broja transakcija zaključenih u elektronskoj formi zahtijeva promptnu reakciju državnog zakonodavstva, kako bi interesi potrošača bili zaštićeni i kako bi se onemogućilo fraudolozno ponašanje pružaoca usluga, čiji je cilj zloupotreba pravnih praznina za sticanje koristi. Bosna i Hercegovina i Republika Srpska u su značajnoj mjeri ispratile evropske tokove u pogledu regulisanja ove materije, te mnoge odredbe evropskih direktiva inkorporisale u svoje zakone – Zakon o zaštiti potrošača Bosne i Hercegovine, Zakon o unutrašnjem platnom prometu Republike Srpske i Federacije Bosne i Hercegovine, Zakon o elektronskom novcu Republike Srpske te Zakon o međunarodnim naknadama za platne kartice, kao i kroz interne propise Centralne banke Bosne i Hercegovine.

Zakon o zaštiti potrošača BiH (Službeni glasnik BiH br. 25/2006 i 88/2015) prvi put uvodi pojmove elektronskog instrumenta plaćanja (u daljem tekstu EIP) kao i elektronskog novca (u daljem tekstu e-novac), te reguliše uslove za njihovo izdavanje, obaveze izdavaoca u pogledu zaštite korisnika, ovlaštenja korisnika i ostale aspekte neophodne za nesmetano odvijanje elektronskog platnog prometa. Članom 70. zakonodavac je definisao elektronske instrumente plaćanja kao instrumente plaćanja na daljinu koji korisniku i vlasniku omogućavaju pristup finansijskim sredstvima na njihovom računu kod neke finansijske institucije, radi obavljanja prenosa novčane vrijednosti (transakcije), prilikom čega se redovno traži identifikacioni broj i/ili sličan dokaz identiteta. Detaljniju definiciju elektronskog novca možemo naći u članu 2. stav 1. tačka 1. Zakona o elektronskom novcu RS (Službeni glasnik Republike Srpske, br. 1/24): elektronski novac označava elektronski (uključujući magnetno) pohranjenu novčanu vrijednost koja čini novčano potraživanje prema izdavaocu tog novca, a izdata je nakon prijema novčanih sredstava radi izvršavanja platnih transakcija i prihvata je fizičko ili pravno lice koje nije izdavalac tog novca, u skladu sa propisom kojim se uređuju elektronski novac, izdavaoci elektronskog novca i nadzor nad njima u Republici Srpskoj, pri čemu elektronski novac ne uključuje digitalni zapis valute koju nije izdala i za čiju vrijednost ne garantuje centralna banka, niti drugi organ javnog sektora i koja nema pravni status novca ili valute.

Zakonom o zaštiti potrošača zabranjuje se izdavaocu EIP da otkriva podatke o kori-

sniku. Odgovor na pitanje ko može biti izdavalac nalazimo u Zakonu o unutrašnjem platnom prometu RS (Službeni glasnik Republike Srpske br. 52/2012, 92/2012 – ispr., 58/2019, 38/2022 i 63/2024), koji u članu 4. stav 1. kaže da su ovlašćene organizacije za obavljanje poslova platnog prometa u smislu ovog zakona banke sa sjedištem u Republici Srpskoj, filijale banaka iz Federacije Bosne i Hercegovine i Brčko Distrikta Bosne i Hercegovine koje imaju dozvolu Agencije za bankarstvo Republike Srpske i drugi subjekti koji obavljaju poslove platnog prometa za ovlašćene organizacije u skladu sa ovim zakonom.

Takođe, Zakon o zaštiti potrošača predviđa obavezu zaključenja ugovora između pružalaca usluga, odnosno ovlašćenih organizacija za vršenje poslova platnog prometa. Na ovaj način zakonodavac apostrofira značaj ovih ugovora za platni promet uopšte i nedostatak forme sankcioniše ništavošću, te na taj način vrši pritisak na ekonomski jaču stranu da postupi savjesno, a na slabiju da detaljno razmotri svoja prava i obaveze koje nastaju iz ovog ugovora. Iako se u najvećem broju slučajeva radi o ugovorima po pristupu na koji korisnik nema velikog uticaja u pogledu bitnih odredaba ugovora, oni ipak moraju biti usklađeni sa prinudnim propisima, javnim poretком i dobrim običajima, čime se jamči pravna zaštita korisnika.

Dalje, u članu 72. Zakona o zaštiti potrošača normirana je obaveza izdavaoca EIP da uputi vlasnika o mjerama koje treba da preduzme u cilju sopstvene zaštite. Ovaj član služi kao osnov za detaljnije uređenje ovog pitanja ugovorom i opštim uslovima, naročito u slučajevima kada izdavalac ne odgovara za štetu. Ukoliko bi vlasnik EIP na istom zabilježio identifikacioni broj ili neku drugu šifru, postupio bi protivno članu 74, koji ovakve postupke izričito zabranjuje, te snosio odgovornost za štetu. Analogno ovoj odredbi, član 75. štiti izdavaoca u slučaju da korisnik ne prijavi gubitak EIP u razumnom roku te postupi sa grubom nepažnjom. Odgovornost izdavaoca u ovom slučaju je isključena za gubitak u iznosu do 300 KM, što je u skladu sa evropskim propisima, o čemu će biti riječi u daljem toku izlaganja. Korisnik nije odgovoran ako je EIP upotrijebljen bez njegovog prisustva ili bez njegove identifikacione kartice. Primjena povjerljive šifre ili drugog identifikacionog sredstva nije dovoljna za njegovu odgovornost. Za troškove nakon prijave gubitka EIP odgovara izdavalac, budući da mu je članom 78. dato ovlaštenje da, čak i ukoliko se korisnik grubo i prevarantski ponaša, ograniči dalje korištenje EIP.

Neophodno je, u cilju razumijevanja ovih zakonskih tokova, napraviti kratak osvrt na najznačajnije pravne akte Evropske unije vezane za ovu, a to su Direktiva 2007/64, u praksi poznatija pod skraćenicom PSD 1.

Direktiva PSD 1 je jedan od prvih dokumenata koji opširno uređuju ovu materiju i predstavlja pravnu nadogradnju tržišne regulative uspostavljene ranijim direktivama EU donesenim krajem prošlog vijeka. Podudarnost ove direktive se našim zakonodavstvom u pogledu EIP je gotovo stopostotna. Neki od primjera za to bili bi sljedeći:

- član 54. PSD 1 propisuje neophodnost saglasnosti platioca za transakciju i moguće povlačenje iste, što je preuzeto u našem pravu
- član 55. PSD 1 ovlašćuje izdavaoca da blokira sredstva zbog sumnjivih transfera pod istim uslovima kao i u prethodno citiranom članu 78. Zakona o zaštiti potrošača
- član 56. PSD 1 preuzet je u članu 75. Zakona o zaštiti potrošača a tiče se obaveze korisnika da bez odlaganja prijavi izdavaocu gubitak sredstva plaćanja
- obaveze iz Člana 57. PSD1 koje se tiču zabrane izdavaocu da otkriva trećim licima podatke o korisniku podudarne su sa obavezama iz člana 76. Zakona o zaštiti potrošača
- članom 61. PSD1 propisuju se uslovi za odgovornost izdavaoca i granični iznos kao u članu 75. Zakona o zaštiti potrošača, s tim da je za evropske okvire taj iznos 150 EUR, što je približni novčani ekvivalent iznosu od 300 KM koji je propisan našim zakonom.

Pored pobrojanih sličnosti, uporednom analizom može se utvrditi još mnogo poklapanja, ali za potrebe ovog rada nije svrsishodno nabrajati sve. Jasno se vidi iz upoređivanja da naše zakonodavstvo prati razvoj prava EU.

Drugi značajan akt, koji se javlja kao nastavak prvog, jeste Direktiva 2015/2366, poznatija kao PSD2. Ona pobliže reguliše materiju i usklađuje je sa modernim tokovima. Kao i sa PSD 1, postoje značajna poklapanja naših propisa sa PSD 2, a neki od njih su:

- Član 52. PSD 2 koji obavezuje izdavaoca da uputi korisnika u zaštitne mjere preuzet je u članu 72. Zakona o zaštiti potrošača
- Član 64. PSD 2 koji se tiče autorizacije preuzet je u internim propisima ovlaštenih izdavalaca
- Član 68. PSD 2 se nadovezuje na Član 55. PSD 1 i preuzet je u našem pravu kao što je već bilo riječi

Takođe značajna odredba jeste odredba člana 72. PSD 2, koja u slučaju kada korisnik tvrdi da je do transakcije došlo bez njegovog odobrenja, a izdavalac tvrdi da jeste, teret dokazivanja da je transakcija autorizovana prebacuje na izdavaoca. Članom 97. PSD 2 regulisana je autentifikacija, pristup putem interneta, blokiranje sumnjivih transakcija i pristup sa sumnjive udaljenosti, o čemu je već bilo riječi u dijelu izlaganja koji se bavi ovim pitanjima.

ANALIZA STUDIJE SLUČAJA

Studija slučaja **PayPal** dodatno potvrđuje da su povjerenje i sigurnost ključni faktori uspjeha digitalnih platnih servisa. PayPal je razvio poslovni model zasnovan na **transparentnosti, sigurnosti i jednostavnosti upotrebe**, čime je uspio da privuče stotine miliona korisnika širom svijeta. Analiza pokazuje nekoliko važnih rezultata:

- **Demokratizacija finansijskih usluga:** PayPal je omogućio pristup digitalnim plaćanjima potrošačima i malim biznisima koji ranije nisu imali priliku da koriste tradicionalne bankarske kanale. Ovaj model doprinio je uključivanju šire populacije u digitalnu ekonomiju, posebno u zemljama u razvoju.
- **Povećanje povjerenja korisnika:** Istraživanja pokazuju da je vjerovatnoća da korisnik završi kupovinu za 57% veća ukoliko je dostupan PayPal kao opcija plaćanja. Ova činjenica proizlazi iz percepcije da PayPal nudi bolju zaštitu od prevara i jednostavniji proces povrata novca u slučaju spora.
- **Sigurnosni mehanizmi:** PayPal primjenjuje napredne tehnologije poput enkripcije, tokenizacije i višefaktorske autentifikacije, čime smanjuje rizik od krađe podataka i neovlaštenog pristupa. Osim tehničkih rješenja, kompanija ulaže i u sofisticirane algoritme za detekciju prevara i pranja novca.
- **Regulatorna saradnja:** PayPal aktivno sarađuje sa regulatornim tijelima u različitim državama, gradeći svoj kredibilitet kao pouzdan i odgovoran pružalac usluga. Poseban akcenat stavlja na usklađenost sa propisima o sprečavanju pranja novca (AML) i finansiranja terorizma, što dodatno učvršćuje povjerenje korisnika i partnera.
- **Globalna ekspanzija i konkurentnost:** kroz akvizicije (npr. kupovina GoPay-a u Kini) i strateška partnerstva, PayPal je proširio svoje prisustvo na ključnim tržištima i ojačao svoj položaj globalnog lidera u elektronskim plaćanjima. Ovakva strategija istovremeno je podigla standarde zaštite potrošača na globalnom nivou.

Ukupno posmatrano, rezultati analize pokazuju da uspješnost elektronskog plaćanja zavisi od kombinacije tehnoloških inovacija, regulatornog okvira i povjerenja potrošača. Dok regulativa postavlja minimalne standarde zaštite, praksa pokazuje da kompanije poput PayPal-a, koje ulažu dodatne napore u sigurnost i korisničku zaštitu, postižu daleko viši stepen prihvatanja i dugoročnu konkurentsku prednost (Porter, 2021).

DISKUSIJA

Dobijeni rezultati ukazuju na to da je razvoj elektronskog plaćanja neraskidivo povezan sa pitanjem sigurnosti i povjerenja potrošača. Literatura potvrđuje da su sigurnost i privatnost podataka, povjerenje korisnika, regulatorne praznine i tehničke barijere najveći izazovi elektronskog poslovanja. Iako pravni okvir pruža institucionalne garancije, on sam po sebi nije dovoljan da bi potrošači imali potpuno povjerenje u digitalne transakcije. Ključnu ulogu imaju informatičke tehnologije, koje kroz mehanizme poput enkripcije, tokenizacije i višefaktorske autentifikacije direktno utiču na bezbjednost i korisničko iskustvo.

Analiza zakonskih akata pokazala je da je naša zemlja uspostavila pravičan balans između interesa izdavaoca EIP i e-novca i interesa korisnika, te na taj način omogućila pravnu sigurnost koja doprinosi sve učestalijem opredjeljenju građana za elektronske vidove plaćanja. Bosna i Hercegovina, uprkos tome što na mnogim poljima zaostaje za Evropskom unijom, u pogledu zaštite potrošača i sigurnosti elektronskih transakcija u potpunosti ju je ispratila i na taj način postala dio jedinstvenog evropskog elektronskog tržišta, što je bilo i očekivano s obzirom na njenu obavezu proisteklu iz Sporazuma o stabilizaciji i pridruživanju da uskladi svoje zakone sa komunitarnim tekovinama.

Studija slučaja PayPal pokazuje kako kombinacija naprednih tehnoloških rješenja i jasnih pravila zaštite korisnika može stvoriti globalno prepoznat i pouzdan servis. PayPal je uspješno izgradio poslovni model u kojem je sigurnost postavljena kao prioritet, što se direktno odrazilo na povjerenje potrošača i na ekonomsku uspješnost platforme. Njegov primjer potvrđuje da tehničke inovacije moraju biti praćene i pravnom sigurnošću – tek tada potrošači razvijaju dovoljno povjerenja da zaista prihvate digitalne servise.

ZAKLJUČAK

Elektronsko plaćanje predstavlja jedan od ključnih stubova digitalne ekonomije, jer omogućava brže, jednostavnije i dostupnije finansijske transakcije u globalnom okruženju. Međutim, rezultati pokazuju da je njegovo uspješno funkcionisanje uslovljeno rješavanjem brojnih izazova, prije svega onih koji se odnose na sigurnost podataka, povjerenje potrošača i usklađenost sa pravnim okvirima.

Zaključci koje možemo izvući iz ovakve analize mogu se sažeti u nekoliko rečenica. Prvi i najbitniji jeste da se Bosna i Hercegovina implementacijom i inkorporisanjem normi EU u svoje zakonodavstvo izjednačila sa standardima zaštite potrošača koji postoje na evropskom tržištu. Takođe, kada se pored zakona uzmu u obzir i podzakonski propisi, kao i opšti akti izdavaoca (najčešće banaka, ali i platformi poput PayPal-a), vidi se velik stepen podudaranja. Ovakve tendencije su prirodna posljedica univerzalnosti današnjeg tržišta i potrebe svih tržišnih takmičara da budu konkurentni, pod jednakim uslovima, svuda.

Studija slučaja PayPal-a pokazala je da je kombinacija naprednih tehnoloških rješenja i jasnih pravnih mehanizama zaštite potrošača ključ za uspjeh na globalnom tržištu. Kroz enkripciju, tokenizaciju, višefaktorsku autentifikaciju i efikasne sisteme detekcije prevara, PayPal je uspio da izgradi visok stepen povjerenja korisnika, što se direktno odražava na njegovu konkurentnost i globalni rast.

Na osnovu sprovedene analize može se zaključiti da budućnost elektronskog plaćanja u BiH i regionu zavisi od paralelnog razvoja sigurnosnih tehnologija i regulatornog okvira. Preporučuje se još jača harmonizacija domaćih zakona sa evropskim standardima, ulaganje u savremena informatička rešenja i kontinuirana edukacija potrošača o sigurnoj upotrebi digitalnih servisa. Samo sinergija poslovne informatike i prava može stvoriti dovoljno sigurno i transparentno okruženje koje će omogućiti dalji rast elektronskog plaćanja i izgradnju povjerenja u digitalnu ekonomiju.

Pristup za koji su se autori odlučili prilikom pisanja ovog rada za svrhu ima pružanje mogućnosti čitaocu da kroz analizu pravne regulative i aktuelnih trendova u digitalnoj ekonomiji razumije odnos između normativnog i stvarnog, te da na taj način percipira nove trendove u platnom prometu i svakodnevnom životu. Iako pravo uvijek zaostaje jedan korak za stvarnim potrebama društva, naročito u vremenu tehnoloških inovacija i ubrzanog napretka u kome živimo, brze reakcije zakonodavaca u pogledu normiranja novih pojava pokazuju koliki značaj digitalna ekonomija ima u savremenom društvu.

LITERATURA

- Dijeh, P., Babu, S., & Vijayalakshmi, Y. (2020). Enhancement of e-commerce security through asymmetric key algorithm. *Computer Communications*, 153, 125–134. <https://doi.org/10.1016/j.comcom.2020.01.033>
- Gupta, H., & Sharma, V. (2011). Role of multiple encryption in secure electronic transaction. *International Journal of Network Security & Its Applications*, 3(6), 89–96. <https://doi.org/10.5121/IJNSA.2011.3606>
- Hassan, M., Shukur, Z., Hasan, M., & Al-Khaleefa, A. (2020). A review on electronic payments security. *Symmetry*, 12(8), 1344. <https://doi.org/10.3390/sym12081344>
- How does payment tokenization work? (2021, April 17). *M2P Blog*. <https://m2pfintech.com/blog/how-does-payment-tokenization-work>
- Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T., & Koucheryavy, Y. (2018). Multi-factor authentication: A survey. *Cryptography*, 2(1), 1. <https://doi.org/10.3390/cryptography2010001>
- Porter, M., Kramer, M., & Lobb, A. (2021). *PayPal: The next chapter*. Harvard Business School. <https://shared-value.org.au/wp-content/uploads/2023/07/HBR-Case-Study-PayPal-The-Next-Chapter.pdf>
- Radenković, B., Despotović-Zrakić, M., Bogdanović, Z., Barać, D., & Labus, A. (2015). *Elektronsko poslovanje*. Fakultet organizacionih nauka. <https://www.elab.fon.bg.ac.rs/wp-content/uploads/2015/07/Elektronsko-poslovanje.pdf>
- Xia, L., Baghaie, S., & Sajadi, M. (2023). The digital economy: Challenges and opportunities in the new era of technology and electronic communications. *Ain Shams Engineering Journal*. <https://doi.org/10.1016/j.asej.2023.102411>.

ELECTRONIC PAYMENT IN DIGITAL ECONOMY AND LEGAL ASPECTS OF CONSUMER PROTECTION IN BOSNIA AND HERZEGOVINA

Authors: MARKO GAJIĆ, Boris Đukić

Email: marko.gajic@student.ef.unibl.org

Mentor: Assist. Prof. Ljubiša Mičić

Faculty of Economics, University of Banja Luka

Faculty of Law, University of Banja Luka

Introduction: Electronic payment is a rapidly growing field of modern financial transactions, relying on technologies such as tokenization, multi-factor authentication, and encryption to ensure security. At the same time, legal regulations (EU directives and national laws) provide consumer protection against misuse, while this paper presents conclusions on the development of electronic payments in the local market.

Aim: The aim of this paper is, on the one hand, to identify key security technologies that enable the safe execution of digital transactions, and on the other hand, to examine the legal framework and the effectiveness of existing regulations.

Materials and Methods: In preparing this paper, the authors used a combination of qualitative and comparative research methods. The analysis of specific platforms is illustrated through a case study (PayPal). The materials include professional literature in the fields of business informatics, finance, and law, as well as applicable legal regulations and European directives.

Results: The research has shown that electronic payments offer significant advantages in terms of transaction speed and availability, but also carry risks related to data security and potential misuse. The analysis of the legal framework indicates that PSD2 and GDPR provide a wide range of mechanisms for consumer protection, while domestic laws in the region often lag in their implementation. From a technical perspective, modern platforms apply advanced security measures such as encryption and multi-factor authentication, which significantly reduce the risk of fraud. The analysis of the PayPal platform shows that global services have more developed protection mechanisms and more transparent policies, while local banks only partially comply with these standards.

Conclusion: Electronic payment is the foundation of the digital economy, but its sustainability depends on the synergy between legal regulation and technological solutions. The analysis has shown that global platforms lead in applying security technologies and transparent rules, while local systems require additional investments and alignment with international standards.

Keywords: electronic payment; digital economy; consumer protection; business informatics; legal regulation