Tamara N. Tasić*

Originalni naučni članak
UDK: 342.738
doi: https://doi.org/10.56461/SPZ_1143
Primljeno: 25. 2. 2025.
Prihvaćeno: 2. 12. 2025.
Online First: 3. 12. 2025.

BALANSIRANJE IZMEĐU INOVACIJA I ZAŠTITE PODATAKA O LIČNOSTI NA PRIMERU *CHATGPT*-A**

Sažetak

Zaštita podataka o ličnosti u doba veštačke inteligencije veoma je intrigantna tema u domaćem pravu i pravu Evropske unije. Četbotovi, poput *ChatGPT*-a, sve češće se primenjuju čime se povećava rizik od zloupotreba i potencijalnih povreda ličnih podataka. U ovom radu definiše se pojam četbotova i sprovodi pregled Opšte uredbe o zaštiti podataka o ličnosti (GDPR). U drugom delu autorka analizira kako *ChatGPT* prikuplja, skladišti i obrađuje lične podatke, a potom se fokusira na prateće rizike inovacija i povrede do kojih može doći upotrebom *ChatGPT*-a. Potom autorka ukazuje na tehnike balansiranja kojima bi se mogao izbeći rizik povrede ličnih podataka, uz analizu GDPR-a i davanje konkretnih predloga za povećanje nivoa usklađenosti u eri digitalnih inovacija.

Ključne reči: zaštita podataka o ličnosti, GDPR, povrede ličnih podataka, četbotovi, *ChatGPT*.

* Master pravnik, advokat, doktorand, Pravni fakultet Univerziteta Union, Beograd, Srbija.

E-mail: *tamaratasiclawyer@gmail.com*
ORCID: *https://orcid.org/0009-0006-0563-4522*

** Rad je osvojio prvu nagradu na konkursu „Dr Stefan Andonović" za najbolji naučni rad u kategoriji mladih istraživača za 2025. godinu na temu „Pravni okvir zaštite podataka o ličnosti – balansiranje između inovacija i zaštite privatnosti", koji su organizovali Institut za uporedno pravo Beograd, Republika Srbija, i Pravni fakultet Univerziteta u Kragujevcu, Republika Srbija.

BALANCING BETWEEN INNOVATION AND DATA PROTECTION USING THE EXAMPLE OF *CHATGPT*

Summary

Personal data protection in the age of artificial intelligence is a very intriguing and new topic in domestic and EU law. The use of innovative chatbots such as *ChatGPT* is becoming increasingly common, which increases the risk of misuse and potential violations of personal data. In this paper, the author defines the concept of chatbots and conducts a review of the General Data Protection Regulation (GDPR). The second part analyzes how *ChatGPT* collects, stores, and processes personal data. The paper also focuses on the risks associated with innovations and possible violations that may occur when using *ChatGPT*. The author also points out balancing techniques that could prevent the risk of personal data breaches, with an analysis of the GDPR, and provides concrete suggestions for compliance.

Keywords: Personal Data Protection, GDPR, Personal Data Breaches, Chatbots, *ChatGPT*.

1. Uvodna razmatranja

U svetu inovacija, četbotovi su relativno novi termin koji postaje sve popularniji u globalnoj komunikaciji. Ljudi koriste četbotove u različite svrhe – za kupovinu, bankarske usluge, dostavu i zdravstvenu zaštitu. Uprkos mnogobrojnim prednostima primene, četbotovi mogu voditi bezbednosnim rizicima, usled čega je potrebno pronaći rešenja kojima se ovakvi rizici mogu izbalansirati i smanjiti.

Jedan od rizika upotrebe ovih modernih programa zasnovanih na veštačkoj inteligenciji jeste povreda ličnih podataka, te ugrožavanje jednog od osnovnih prava predviđenog čl. 1, st. 1 Opšte uredbe o zaštiti podataka o ličnosti (General Data Protection Regulation - GDPR) i čl. 4, st. 1, tač. 1 Zakona o zaštiti podataka o ličnosti - ZZPL. GDPR predviđa da je podatak o ličnosti svaki podatak koji se odnosi na fizičko lice čiji je identitet određen ili odrediv. Time je data široka definicija ličnih podataka, čime se proširuje i potencijalni opseg povreda do kojih može doći u praksi.

Upotreba novih tehnologija zasnovanih na veštačkoj inteligenciji povećava broj rizika, te je potrebno detaljno proučiti svaki od njih i dati preporuke kako bi se preventivno reagovalo u slučaju opasnosti. Imajući u vidu da moderni četbotovi

više nisu zasnovani na svojevrsnim pravilima, nego na upotrebi prirodnog jezika i mašinskog učenja, njihov način funkcionisanja i interakcije sa korisnicima potpuno se menja. Takve tehnike podrazumevaju učenje kroz konverzaciju, što povećava mogućnost povrede podataka o ličnosti.

U ovom radu, autorka će se osvrnuti na okolnosti pod kojima četbotovi mogu koristiti podatke o ličnosti, načine obrade tih podataka i potencijalne povrede do kojih može doći. Jedan od ciljeva rada jeste pravljenje detaljne studije o sigurnosnim aspektima u komunikaciji sa četbotovima i ukazivanje na probleme skladištenja tih podataka u doba digitalnih inovacija. Autorka nastoji da pruži odgovarajuće preporuke za izbegavanje povrede ličnih podataka u komunikaciji sa četbotovima i objasni na koji način se može postići balans između razvoja inovacija i zaštite podataka o ličnosti.

2. Pojam i značaj četbotova

Četbotovi ili samo botovi su aplikacije koje ulaze u interakciju sa ljudima pomoću korisničkih komandi. Interakcija se obavlja putem glasovne ili tekstualne konverzacije (Hasal *et al*., 2021, p. 1).[1]

Četbotovi su dizajnirani da funkcionišu nezavisno od ljudi, pokušavajući da razumeju upite i obezbede odgovarajuće odgovore. Moderni četbotovi istovremeno uče iz konverzacije putem mašinskog učenja kako bi obezbedili bolje odgovore u budućnosti (Hasal *et al*., 2021, p. 1).[2]

Velike tehnološke kompanije, kao što su *Google*, *Mete* i *IBM*, doprinele su razvoju četbotova istraživanjima u istom pravcu. To je bilo moguće s obzirom na to da ove kompanije imaju pristup ogromnim setovima podataka na kojima se ovi programi mogu trenirati. Neki od najpopularnijih četbotova u današnje vreme su *Siri*[3] kompanije *Apple*, *Cortana* korporacije *Microsoft* i *Alexa* (proizvod firme *Amazon*).[4]

[1] Prvi primer četbota evidentiran je još 1966. godine kada je Joseph Weizenbaum napravio kompjuterski program koji je pokazivao mogućnosti komunikacije između čoveka i kompjutera primenom prirodnog jezika (Hasal *et al*., 2021, p. 1).

[2] Četbotovi su i adekvatna sredstva za poboljšanje korisničkog iskustva, te se prepoznaje i veća spremnost za njihovu upotrebu, kao i benefiti poput neprekidno dostupne korisničke podrške, personalizovane interakcije i odsustva čekanja. Osim toga, značajni su i za kompanije s obzirom na to da mnogi procesi mogu da se automatizuju, a zaposleni sačuvaju za kompleksnije zadatke.

[3] U teoriji je prisutan stav da konverzacijski četbot *Siri* nije stvoren da oponaša ljudsku inteligenciju i time bolje razume kognitivne procese. Uistinu, *Siri* koristi baze podataka zasnovane na prirodnom jeziku, ali sama aplikacija ima više zajedničkih elemenata sa tradicionalnom oblasti informacionih tehnologija nego sa teorijom kognitivnih sistema za traženje informacija (Cecconi, 2023, p. 2).

[4] Navedeni primeri četbotova funkcionišu po sistemu otvorenih modela koji mogu da učestvuju u bilo kojoj konverzaciji i da razumeju tekst i govor. Tako korisnici mogu zatražiti od

Predmet ovog rada je *ChatGPT*, popularan četbot koji pripada kategoriji konverzacijske tehnologije koja trenutno doživljava veliku ekspanziju u društvu i organizacijama (Sen, Uygun & Erden, 2023, p. 370).[5]

Četbotovi koriste veliki broj baza podataka i čak uče iz tih podataka, što može dovesti do bezbednosnih problema jer korisnici ne znaju kako se njihovi osetljivi podaci obrađuju, dele i skladište. Dodatni problem je činjenica da je Evropska unija više okrenuta ka potrebi regulacije veštačke inteligencije, a manje ka inovaciji, što je potencijalan problem za tržište gde većina najuspešnijih kompanija u ovoj oblasti dolazi iz Amerike i Kine (Mathis & Tor, 2022, p. 177).

Evropski parlament je nedavno usvojio Uredbu o veštačkoj inteligenciji (Artificial Intelligence Act - AI Act). Uredba je stupila na snagu 1. avgusta 2024. godine, sa ciljem da promoviše odgovoran razvoj u oblasti veštačke inteligencije. Ovim dokumentom nastoji se da se obezbede jasne instrukcije i zahtevi koji se tiču primene nove tehnologije, čime se smanjuju rizik i finansijska opterećenja za poslovni sektor. Uredba pominje četbotove samo na jednom mestu, naglašavajući njihovu ulogu kao posrednika u pružanju usluga, a u okviru sistema veštačke inteligencije.[6]

AI Act dalje naglašava obavezu subjekata koji uvode sisteme veštačke inteligencije da detektuju i otklone rizike do kojih može doći širenjem sadržaja koji je generisan putem veštačke inteligencije. Ovde se posebno naglašavaju rizik i negativni efekti na demokratske procese, izbore i opšte dezinformisanje (AI Act, čl. 120). Veliki četbotovi, poput *ChatGPT*-a, već su započeli proces usklađivanja sa Uredbom (A Primer on the EU AI Act, 2024, p. 1), što je njihova obaveza u svetlu uspostavljanja ravnoteže između inovacija i zaštite podataka korisnika.

U pozitivnom pravu Srbije još uvek se čeka na usvajanje Zakona o veštačkoj inteligenciji, čime bi se postigla harmonizacija sa pravom Evropske unije. U međuvremenu, Vlada Republike Srbije je usvojila Etičke smernice za razvoj, primenu i upotrebu pouzdane i odgovorne veštačke inteligencije (Vlada Republike Srbije, 2023, pp. 1-41). Osnov za donošenje ovog dokumenta nalazi se u Strategiji razvoja veštačke inteligencije u Republici Srbiji za period 2020–2025. (Vlada Republike Srbije, 2019, pp. 1-61), a jedan od ciljeva je etička i bezbedna primena veštačke

četbotova da im kontrolišu kućne uređaje, reprodukuju muziku, upravljaju imejl listom i kalendarima, obavljaju mnoge druge zadatke, i tako spoznati prednosti ovih inovativnih modela.

[5] Mnogi autori govore o potrebi stvaranja inovativne teorije imajući u vidu mogućnosti *ChatGPT*-a da generiše nove ideje i kreativna rešenja, a što je ključ njegove korisnosti (Sen, Uygun & Erden, 2023, p. 372).

[6] Na osnovu Uredbe, sistemi veštačke inteligencije mogu se upotrebljavati za pružanje internet pretraga, posebno u meri u kojoj sistem, kao što je internet četbot, u načelu pretražuje sve internet stranice, zatim uključuje rezultate u svoje postojeće znanje i upotrebljava nadopunjeno znanje kako bi generisao jedan izlazni rezultat koji objedinjuje različite izvore informacija (AI Act, čl. 119).

inteligencije. U međuvremenu, usvojena je i Strategija razvoja veštačke inteligencije u Republici Srbiji za period 2025–2030, koja pominje značaj i rasprostranjenost *ChatGPT*-a kao sistema generativne veštačke inteligencije koji se upotrebljava u svakodnevnom životu (Vlada Republike Srbije, 2025, pp. 1-61).[7]

Treba uzeti u obzir činjenicu da domaća regulativa još uvek nije potpuno revidirana, čime bi se omogućila bezbedna i olakšana primena veštačke inteligencije. To se posebno odnosi na pravila upravnog postupka koje je potrebno inovirati, kako bi se stvorio osnov za korišćenje veštačke inteligencije (Andonović, 2020, p. 151).

3. Način prikupljanja, upravljanja i skladištenja podataka korisnika putem *ChatGPT*-a

Da bismo mogli da razumemo bezbednosne probleme i rizike u pogledu zaštite podataka o ličnosti, najpre je potrebno analizirati na koji način ovi modeli koriste i skladište podatke. *ChatGPT* prikuplja podatke korisnika u različitim fazama interakcije, što je definisano u politici privatnosti same kompanije. Najpre, to uključuje lične podatke koje obezbeđuje korisnik, poput informacija o nalogu, sadržaj koji korisnik unese u pretraživač, informacije podeljene mejlom ili na društvenim mrežama i podatke prikupljene u istraživanjima.

Sledeća grupa informacija koje *ChatGPT* prikuplja jesu podaci koji proizlaze iz upotrebe samih usluga kompanije.[8] Naposletku, *ChatGPT* prikuplja informacije putem trećih izvora, uključujući pouzdane i bezbednosne partnere, kojima pomaže pri zaštiti protiv prevare, zloupotreba i drugih bezbednosnih pretnji.

Kada je u pitanju skladištenje, *ChatGPT* zadržava lične podatke korisnika samo onoliko koliko je potrebno radi pružanja usluga ili u druge legitimne poslovne svrhe kao što su rešavanje sporova, bezbednosni razlozi ili poštovanje zakonskih obaveza.[9] *ChatGPT* takođe ističe da korisnici mogu imati određena prava u vezi sa ličnim podacima, a u zavisnosti od domaće jurisdikcije.[10]

[7] U Strategiji se takođe ističe da, uprkos svim koristima do kojih može doći u oblasti veštačke inteligencije, postoje i prateći izazovi koje je neophodno sagledati i uzeti u obzir u daljem planu razvoja. Jedno od delikatnih pitanja jeste i zaštita podataka o ličnosti i kako sprečiti zloupotrebu ovih tehnologija i obezbediti uslove za zaštitu privatnosti podataka (Vlada Republike Srbije, 2019, p. 7).

[8] Kada korisnik poseti sajt, kompanija prikuplja podatke koje njen pretraživač automatski šalje (*log data*), informacije o načinu upotrebe usluga, tip sadržaja koji korisnik posećuje i radnje koje preduzima s tim u vezi (*usage data*), podatke o korišćenom uređaju, lokaciji i kolačiće.

[9] Vremenski period čuvanja ličnih podataka zavisiće od brojnih faktora kao što su svrha obrade podataka, količina, priroda i osetljivost informacija, potencijalni rizik od štete usled neovlašćene upotrebe ili otkrivanja, ili obavezujući pravni zahtev.

[10] Taksativno su nabrojana sledeća prava korisnika: pristup ličnim podacima i informacijama

Sumirajući načine obrade, prikupljanja i skladištenja podataka od strane *ChatGPT*-a, može se zaključiti da se kompanija pridržava osnovnih načela iz čl. 5 GDPR-a. Pod tim podrazumevamo načela zakonitosti, svrsishodnosti, minimizaciju podataka, tačnosti, ograničenje čuvanja, integriteta i odgovornosti za postupanje. Ista načela predviđena su i čl. 5 ZZPL-a.

GDPR u čl. 5, st. 2 predviđa da se podaci o ličnosti mogu prikupljati u svrhe koje su konkretno određene, izričite, opravdane i zakonite i dalje se oni ne mogu obrađivati na način koji nije u skladu sa tim svrhama. Imajući u vidu prethodno navedeno, način na koji *ChatGPT* prikuplja i obrađuje lične podatke može se okarakterisati kao opravdan i zakonit,[11] ili se bar može reći da usklađenost poslovanja ovog četbota egzistira „na papiru". Da li se kompanija pridržava ovih načela, pitanje je u svakom pojedinačnom slučaju. Ovo stoga što je politika privatnosti kompanije podložna promenama te nije jasno da li se *ChatGPT* u potpunosti pridržava pojedinih načela, poput svrsishodnosti (Naghiyev, 2024, p. 9).

Kada je u pitanju vremenski rok skladištenja podataka, autorka smatra da su osnovi čuvanja opravdani i da kompanija legitimno određuje faktore od kojih zavisi rok čuvanja ličnih podataka. To upućuje na usklađenost sa načelom „ograničenja čuvanja", a na osnovu kog se podaci o ličnosti moraju čuvati u obliku koji omogućava identifikaciju lica samo u roku koji je neophodan za ostvarivanje svrhe obrade (GDPR, čl. 5, st. 1).[12] Jasno je da GDPR sprečava *ChatGPT* da pohranjuje lične podatke korisnika duže nego što je to potrebno. S druge strane, produženo skladištenje tih podataka u javnom interesu bilo bi moguće, na primer u slučaju da je reč o podacima koji su bitni za otkrivanje teških krivičnih dela protiv javne bezbednosti (Krivični zakonik RS, 2005, čl. 322-354).

Proizvođači četbotova prepoznaju potrebu usklađivanja sa propisima GDPR-a. Tako su mnoge kompanije omogućile funkcije poput „zahtevaj lične podatke", „obriši lične podatke" ili „izmeni lične podatke". *ChatGPT* ne zaostaje za ovim trendovima, te kompanija omogućava korisnicima da izbrišu svoje podatke u interfejsu ili da podnesu zahtev za brisanje naloga, što će operator sprovesti u roku od 30 dana (How to delete your account, n.d.).

---

o tome kako se obrađuju; brisanje ličnih podataka iz evidencije; ažuriranje ili ispravka ličnih podataka; prenošenje ličnih podataka trećoj strani; ograničenje načina na koji se obrađuju lični podaci; povlačenje saglasnosti za obradu podataka; osporavanje načina obrade ličnih podataka i podnošenje žalbe nacionalnom organu za zaštitu podataka.

[11] Postavlja se pitanje šta se podrazumeva pod principom zakonitosti i kada prikupljanje podataka ispunjava te svrhe. Čini se da je legitimnost slična društvenom interesu budući da se ove dve sfere umnogome preklapaju. Postojanje društvenog interesa u velikom broju slučajeva je i uslov za obrađivanje podataka o ličnosti na legitiman (zakonit) način (Milić, 2020, p. 50).

[12] Ipak, prekoračenje ovog pravila je moguće ako se skladištenje podataka vrši u javnom interesu, u svrhe naučnog i istorijskog istraživanja, arhivske ili statističke svrhe. U tom slučaju organizacija bi morala da obezbedi odgovarajuće tehničke mere radi zaštite ličnih podataka.

Ovde treba naglasiti da *ChatGPT* ne briše podatke (upite) automatski nakon 30 dana, već je potrebno podneti poseban zahtev da se podaci obrišu kako bi rok od 30 dana počeo da teče. Čini se da je kompanija ovde nedovoljno transparentna, te podaci lako mogu biti predmet povrede ukoliko neko upadne u korisnički nalog, a informacije nisu uklonjene zbog neadekvatne informisanosti korisnika.

Čini se da bi kompanija mogla da preduzme odgovarajuće mere u cilju informisanja korisnika o svojoj praksi. Korisno bi bilo, na primer, da *ChatGPT* posle svakog završenog upita upozori korisnike da će njihova pitanja i uneti dokumenti biti pohranjeni, te da im omogući da ih obrišu jednim klikom. To bi se moglo postići jednostavnim *pop-up* obaveštenjem pre nego što korisnik napusti interfejs programa.

Kada su u pitanju prava korisnika u vezi sa ličnim podacima, *ChatGPT* je uskladio politiku privatnosti sa pravima korisnika predviđenim u čl. 15 GDPR-a i omogućio korisnicima da ostvare svoja prava u skladu sa propisima predviđenim nacionalnim zakonodavstvom.

4. Načini povrede ličnih podataka i rizici upotrebe *ChatGPT*-a

Veliki jezički modeli (*Large Language Models - LLM*) poput *ChatGPT*-a proizvode tekst na osnovu obimnog treninga, što može dovesti do rizika po lične podatke, posebno ako generiše odgovore koji otkrivaju osetljive informacije. Imajući u vidu da korisnici sve više upotrebljavaju četbotove u procesu odlučivanja, rizik njihove upotrebe se povećava (Zarifis *et al*., 2024, p. 78).

U ovom delu rada analiziraju se neki od uobičajenih problema koji se odnose na privatnost podataka i njihovo eventualno „curenje" do čega može doći usled primene *ChatGPT*-a u eri digitalnih inovacija:[13]

1. **Nenamerno deljenje osetljivih informacija.** Ovo se dešava kada korisnik nesvesno deli lične ili osetljive podatke sa sistemom. Na primer korisnik bi mogao deliti informacije o svojoj kreditnoj kartici, pouzdajući se u sigurnost programa. Dok modeli kao što je *ChatGPT* nemaju mogućnost pohranjivanja ove informacije, budući da sistem skladišti informacije samo privremeno, do 30 dana, podaci bi potencijalno mogli biti presretnuti tokom prenosa ako komunikacioni kanal nije bezbedan.
2. **Curenje podataka kroz izlaze modela**. Iako *ChatGPT* ne zna specifičnosti podataka na kojima je obučen, ponekad može da generiše odgovore koji izgledaju kao

[13] Povreda privatnosti i bezbednosti podataka narušava reputaciju i korisnost sistema veštačke inteligencije i može dovesti do toga da korisnici izgube poverenje u njih (Choudhury & Shamszare, 2023, p. 6).

da se pozivaju na određene podatke ili otkrivaju osetljive informacije. Međutim, ovi odgovori se generišu na osnovu obrazaca naučenih tokom obuke i ne odražavaju pristup bilo kakvim poverljivim bazama podataka. Program bi mogao da „halucinira" specifične, osetljive detalje u odgovorima.[14] Izgleda da veštačka inteligencija nije nepristrasna, mada se ljudi retko osvrću i na moguće negativne strane njene upotrebe (Avramović & Jovanov, 2023, p. 163).

3. **Neprijateljski napadi.** Ovi napadi uključuju zlonamerne aktere koji pokušavaju da manipulišu ili prevare sistem da se ponaša na određeni način, obično u štetne svrhe. Na primer, napadač bi mogao uneti u sistem pažljivo izrađene podatke dizajnirane da ga prevare kako bi program generisao štetan sadržaj. Neki od sajber bezbednosnih napada na *ChatGPT* uključuju napade izbegavanja, trojanske napade i slično (Sebastian, 2023, p. 6).

Ako analiziramo navedene načine povrede ličnih podataka korisnika, možemo videti da je samo prvi – nenamerno deljenje osetljivih informacija – radnja „nesvesne" prirode, dok su ostale radnje povezane sa spoljnim rizicima kada se kao napadač javlja treće lice.

Ovde se postavlja pitanje bezbednosti *ChatGPT*-a, odnosno da li je sistem dovoljno bezbedan od potencijalnih rizika, te da li se može odbraniti u slučaju napada. Sistemske ranjivosti su slabosti koje napadač može iskoristiti da bi izvršio neovlašćene radnje unutar računarskog sistema. Sistem je ranjiv kada ima slabo kodiranje, nedostaju mu aktuelni drajveri na hardverskoj strani ili ima slab zaštitni zid.

U GDPR-u se navodi da svaka tehnologija koja koristi lične podatke korisnika mora da održava strogu bezbednost kako ne bi došlo do zlonamerne aktivnosti koja dovodi do povrede ličnih podataka. Svaki inovativni sistem ili softver mora osigurati alternativne opcije ako dođe do slučajnog ili nezakonitog uništavanja ličnih podataka, neovlašćenog otkrivanja ličnih podataka i njihovog prenosa. Stoga svaki četbot mora da ima „odgovarajuće mere zaštite" da bi izbegao bezbednosne izazove zasnovane na šifrovanju, a u skladu sa čl. 89 GDPR-a. Ovo je tipičan primer kako Uredba, zahtevajući visok nivo bezbednosti modela, želi da izbalansira uticaj četbotova na zaštitu podataka o ličnosti.[15]

Pitanje je šta se dešava u međuvremenu, te da li kompanija transparentno obaveštava korisnike kako su tretirani njihovi podaci uneti tog dana ili u vremenskom periodu koji se podudara sa napadom na servis. Činjenica je da korisnici imaju

[14] Međutim, model ne daje osetljive odgovore, tj. podatke iz stvarnog sveta koje je naučio tokom treninga – on pravi stvari na osnovu obrazaca koje je naučio (Alkaissi & McFarlane, 2023, p. 3).

[15] Često smo svedoci da dolazi do pada velikih sistema kao što su Mete, Instagram, X, te ni *ChatGPT* nije izuzet iz ove prakse. Tako je i *ChatGPT* iskusio pad sistema kada je iscureo veliki broj podataka, te su se upiti pojedinih korisnika pojavljivali u interfejsu drugih (March 20 ChatGPT outage: Here's what happened, 2023, p. 1).

malo koristi od saopštenja, te je potrebno preduzeti konkretne zaštitne mere. To podrazumeva preduzimanje mera tehničke zaštite i testiranje ranjivosti sistema na potencijalne neprijateljske napade. Testiranjem bezbednosti sistema lako bi se mogle uočiti ranjivosti i reagovalo bi se preventivno da do ovakvih rizika ne dođe.

Kada je u pitanju sigurnost *ChatGPT*-a, kompanija je tačno precizirala nivo bezbednosti korisnika u politici privatnosti. Prema zvaničnom tekstu, kompanija primenjuje komercijalno razumne tehničke, administrativne i organizacione mere u cilju zaštite ličnih podataka od gubitka, zloupotrebe i neovlašćenog pristupa, otkrivanja, izmene ili uništenja. Međutim, ističe se da nijedan prenos putem interneta ili elektronske pošte nikada nije potpuno bezbedan ili bez grešaka, te je potrebna posebna pažnja pri odlučivanju koje informacije korisnici pružaju modelu.[16]

ChatGPT takođe navodi da nije odgovoran za zaobilaženje postavki privatnosti ili bezbednosnih mera sadržanih u servisu ili veb lokacijama trećih strana. Postavlja se pitanje da li je time kompanija OpenAI, koja stoji iza *ChatGPT*-a, u potpunosti ograničila svoju odgovornost od mogućih povreda do kojih može doći nesvesnim unosom podataka od strane korisnika i prebacila je na treća lica (fizička lica ili odgovorna lica u pravnom licu), insistirajući na posebnoj pažnji.

Uzmimo fiktivni primer zaposlenog koji unese lične podatke klijenta u *ChatGPT*, a dođe do curenja podataka usled čega oni postanu dostupni trećim licima. Pitanje odgovornosti usled unosa ovih podataka zavisiće od okolnosti svakog slučaja. Ukoliko je *ChatGPT* preduzeo mere predostrožnosti, uključujući nivo bezbednosti sistema da do curenja ne dođe, te se pridržavao odredaba GDPR-a, teret dokazivanja bio bi na suprotnoj strani (na licu koje je unelo podatke). Time se otvara pitanje odgovornosti zaposlenog koji je uneo te podatke u sistem, te odgovornosti kompanije čija je obaveza da edukuje zaposlenog u vezi sa upotrebom generativnih modela.[17]

Kada su u pitanju domaći propisi, na potencijalni slučaj povrede primenjuje se čl. 170, st. 1 Zakona o obligacionim odnosima, kojim je predviđeno da za štetu koju zaposleni u radu ili u vezi sa radom prouzrokuje trećem licu odgovara preduzeće u kome je zaposleni radio u trenutku prouzrokovanja štete, osim ako dokaže

[16] Ovde treba imati u vidu da *ChatGPT* i slični programi prave greške i da oni nisu savršeni pa je jasna suzdržanost kompanije u pogledu davanja bilo kakvih garancija bezbednosti. Jasno je da rad četbotova i stvaranje nesumnjivo falsifikovanog sadržaja (*Deep Fake*) od strane algoritma može uticati na sposobnost pojedinca da izgradi stavove na pouzdanim informacijama. Na taj način se njima manipuliše i ugrožava pravo da budu informisani kako bi učestvovali u procesima demokratskog odlučivanja (Gasmi & Prlja, 2021, p. 326).

[17] Ukoliko je kompanija unela jasnu odredbu u ugovor o radu kojom se zabranjuje upotreba digitalne tehnologije i sistema veštačke inteligencije u vezi sa radom, odgovornost usled curenja podataka biće na zaposlenom. U ovom slučaju kompanija bi takođe mogla biti solidarno odgovorna sa zaposlenim, a u zavisnosti od ugovornih odredaba i okolnosti svakog slučaja.

da je zaposleni u datim okolnostima postupao onako kako je trebalo. Međutim, oštećenik (kompanija) ima pravo zahtevati naknadu štete i neposredno od radnika ako je štetu prouzrokovao namerno (ZOO, čl. 170, st. 2). Ova odredba je u skladu sa načelom ravnopravnosti (ZOO, čl. 11) dveju strana u obligacionom odnosu, te načelom savesnosti i poštenja (ZOO, čl. 12) kojeg bi se obe strane morale pridržavati.

5. Izbegavanje rizika i mere jačanja zaštite podataka o ličnosti

Kao što smo videli, povrede ličnih podataka usled upotrebe *ChatGPT*-a su moguće, te je potrebno razmišljati o prevenciji kako bi se izbegle ozbiljne povrede u praksi. Mogući načini otklanjanja i balansiranje takvih rizika, a primenom odgovarajućih mera zaštite, jesu:

1. **Anonimizacija i agregacija podataka.** Anonimizacija je metod zaštite podataka gde se informacije za ličnu identifikaciju zamenjuju veštačkim identifikatorima. Značajno je razlikovati anonimizaciju podataka od pseudonimizacije, jer kada se podaci anonimiziraju, oni više ne predstavljaju lične podatke, pa prestaje potreba za njihovom zaštitom (Andonović, 2019, p. 311).[18]
2. **Ograničavanje brzine i blokiranje automatizovanih upita.** Ograničavanje brzine uključuje ograničavanje broja zahteva koje korisnik može uputiti sistemu u određenom vremenskom periodu. Blokiranje automatizovanih upita je još jedna mera koja može biti implementirana da zaštiti sistem od automatizovanih napada ili zloupotreba (Sebastian, 2023, p. 9).

Jedan od najlakših načina za zaštitu podataka korisnika jeste prethodno navedena anonimizacija podataka. *ChatGPT* bi morao da razmišlja o davanju preporuka korisnicima ili prikazivanju svojevrsnog *disclaimer*-a koji bi korisnicima savetovao da zaštite lične podatke anonimizacijom pre njihovog deljenja sa botom. Time bi se znatno smanjila mogućnost povrede ličnih podataka kroz podizanje svesti korisnika. Sličan sistem mogla bi da implementira i sama kompanija putem softvera koji bi automatski detektovao lične podatke i aktivirao proces anonimizacije.

Potreba redovnog nadzora nad *ChatGPT*-om je jasna kada se uzmu u obzir ozbiljni propusti koje je kompanija učinila u svom poslovanju. Jedan od spornih slučajeva je registrovan u Italiji, kada je nacionalni organ za zaštitu podataka našao da je kompanija prekršila pravila koja se tiču zaštite podataka. Istraga je utvrdila kršenja odredbi sadržanih u GDPR-u, a koje se tiču masovnog prikupljanja podataka korisnika koji se zatim koriste za obuku algoritma. Kompanija se branila da

[18] Agregacija, s druge strane, uključuje kombinovanje podataka na način na koji rezultirajući skup podataka ne sadrži lične informacije (Puranjay Savar, 2023, p. 437).

aktivno radi na smanjenju ličnih podataka u obuci sistema, koji odbija zahteve za privatne ili osetljive informacije (Rahman-Jones, 2024, p. 1).[19]

Iz primera Italije jasno se može videti da *OpenAI* ponekad krši načelo minimizacije te prikuplja više podataka nego što je to potrebno da bi se sistem trenirao. Ovaj sporan slučaj i zabrana mogli su se izbeći da je *ChatGPT* u početku koristio samo neophodne podatke za obuku algoritma, te adekvatno informisao korisnike i državne organe o svojoj praksi.

Sličan primer je registrovan u Holandiji, gde je radnik medicinske ordinacije uneo medicinske podatke o pacijentu u četbot suprotno uputstvima svog poslodavca, te primer telekomunikacione kompanije čiji je zaposleni uneo u četbot datoteku sa podacima kupaca, uključujući njihove adrese (Nauwelaerts, 2024, p. 1).[20]

U ovom slučaju, do same povrede ne bi došlo da je sam četbot automatski anonimizirao unete podatke i preventivno reagovao sa ciljem zaštite ličnih podataka. To ukazuje na tehnički nedostatak sistema i na potrebu razvoja algoritma koji bi ovakve podatke detektovao i maskirao, čime se ne bi ni aktivirao problem odgovornosti nesavesnog korisnika koji unosi lične podatke.

U sferi sve većeg prelaska na automatizovana rešenja i novu tehnologiju, mogu se očekivati daleko veće povrede ličnih podataka koje bi mogle dovesti do ozbiljnih rizika.[21] Zbog toga je potrebna posebna edukacija zaposlenih o rizicima koje nosi *ChatGPT* i kako izbalansirati upotrebu programa sa zaštitom podataka u praksi.

6. *ChatGPT* i nivo usklađenosti sa GDPR-om

Imajući u vidu da četbotovi imaju pristup sve većem broju podataka, za analizu mehanizama zaštite od posebnog značaja je GDPR, kojim se predviđa pravo na privatnost i slobodu zaštite ličnih podataka od zlonamernih povreda. Zlonamerno korišćenje obuhvata neregulisano skladištenje podataka, autentifikaciju, autorizaciju i šifrovanje bez dozvole korisnika.

[19] Italija je bila prva zapadna zemlja koja je blokirala *ChatGPT*, u martu 2023. godine, usled zabrinutosti za privatnost podataka. *ChatGPT* je ponovo uspostavljen oko četiri nedelje kasnije, nakon što je navedeno da je uspešno „rešio ili razjasnio" pitanja koja je pokrenuo nacionalni organ.

[20] Iako se ne navodi da li je to bio *ChatGPT*, izvesno je da je ovo još jedan primer neopreznog korisnika koji nije svestan rizika koji četbotovi donose. Moguće je da se korisnik potpuno pouzda u bezbednost takvog sistema, a do curenja informacija dođe zbog toga što je neki podatak unesen, a sistem je bio u fazi ranjivosti ili nije imao adekvatne zaštitne mere.

[21] Tipičan primer su osiguravajuća društva koja, s obzirom na prirodu svog posla, prikupljaju sve podatke koji bi se mogli podvesti pod kategoriju ličnih. Osiguravajuća društva te podatke moraju da obrađuju kako bi vršila svoju delatnost (Tošić & Novaković, 2020, p. 95).

GDPR se primenjuje samo na kompanije sa sedištem u EU ili u slučaju kada se obrađuju lični podaci građana EU. *ChatGPT* mora biti usklađen sa odredbama Uredbe i kompanija to jasno navodi u sekciji „Sigurnost i privatnost".[22] *ChatGPT* ostavlja slobodu korisnicima da ostvare svoja prava u skladu sa nacionalnim zakonodavstvom, ali je pitanje koliko je ova oblast regulisana u pojedinim državama, te vrlo često može doći do nastanka pravnih praznina i narušavanja pravne sigurnosti.

GDPR u čl. 4 definiše „lične podatke" kao svaku informaciju koja se odnosi na fizičko lice čiji je identitet određen ili odrediv, neposredno ili posredno, posebno na osnovu oznake identiteta kao što su ime i identifikacioni broj, podataka o lokaciji, identifikatora u elektronskim komunikacionim mrežama ili jednog, odnosno više obeležja fizičkog, fiziološkog, genetskog, mentalnog, ekonomskog, kulturnog i društvenog identiteta fizičkog lica. Na osnovu ovakve definicije jasno je da do povrede ličnih podataka može doći u mnogim slučajevima. Međutim, postavlja se pitanje kako *ChatGPT* može da preduzme odgovarajuće mere kojima bi omogućavao neutralne odgovore jer korisnik, kao običan laik, nikad ne može biti dovoljno pažljiv da predvidi šta se sve podrazumeva pod ličnim podatkom. Čini se da bi *ChatGPT* ovde mogao da se stara o većoj usklađenosti putem testiranja odgovora, a potom i njihove evaluacije, nastojeći da balansira između svog inovativnog algoritma i zaštite podataka.

GDPR definiše principe i zakonske osnove za obradu ličnih podataka i precizira pravo na transparentnost u obradi podataka, minimiziranje podataka, ograničenje svrhe, ograničenje skladištenja i preuzimanje, promenu i uklanjanje svih podataka korisnika. Pitanje je koliko su korisnici svesni ove mogućnosti, jer su takva prava uglavnom nevidljiva na prvi pogled, te je često potrebno kontaktirati korisničku podršku radi njihovog korišćenja. To ukazuje da bi kompanija morala da poveća nivo transparentnosti, omogućavajući korisnicima da budu svesni svojih prava i načina na koje ih mogu ostvariti.

Kada je u pitanju načelo minimizacije, *ChatGPT* bi trebalo da implementira napredni nivo zaštite. To se može postići razvojem algoritma koji bi analizom svih podataka izdvojio samo relevantne informacije, isključujući obradu ličnih podataka, posebno u procesu treninga (Goldsteen *et al*., 2022, p. 477).[23]

[22] Kompanija takođe navodi usklađenost sa pozitivnim propisima CCPA (California Consumer Privacy Act), zakonom koji se u Sjedinjenim Državama odnosi na podatke i privatnost stanovnika Savezne Države Kalifornije.

[23] Postoje autori koji ukazuju da je pravo na brisanje u smislu GDPR-a praktično nemoguće ostvariti, jer podaci samim unosom postaju predmet treninga modela i učenja *ChatGPT*-a (Villaronga, Kieseberg, & Li, 2018, p. 306). Ovakvo gledište je naizgled ispravno jer kompanija ne preduzima konkretne mere kako bi upozorila korisnike da će njihovi unosi biti predmet treninga algoritma. Čini se da bi *ChatGPT* ovde mogao da aktivira dodatnu notifikaciju koja bi informisala korisnike o ovoj praksi pre nego što kreiraju nalog.

Kada je u pitanju proces treniranja *ChatGPT*-a, kompanija omogućava korisnicima da isključe opciju kojom se svaki upit korisnika upotrebljava za treniranje sistema. Time se korisniku omogućava da ograniči kompaniju u pogledu načina korišćenja podataka (Data Controls FAQ, n.d.). Jasno je da korisnici možda nisu svesni ove mogućnosti, pa sve dok oni ne isključe tu opciju, *ChatGPT* će koristiti sve unose u cilju treninga modela.[24]

GDPR u čl. 9 takođe predviđa zaštitu podataka o etničkom poreklu i seksualnoj orijentaciji fizičkih lica. Postavlja se pitanje da li je *ChatGPT* u mogućnosti da zaštiti takve podatke u komunikaciji sa korisnikom, što je teško verovati. Potencijalno rešenje u tom slučaju bilo bi generisanje konzistentnih odgovora na upite koji su jezički isti (Sebastian, 2023, p. 9). Ovo rešenje je, međutim, u suprotnosti sa odredbom čl. 22 GDPR-a kojim se predviđa da lice na koje se podaci odnose ima pravo da se na njega ne primenjuje odluka doneta isključivo na osnovu automatizovane obrade, uključujući i profilisanje, ako se tom odlukom proizvode pravne posledice po to lice ili ta odluka značajno utiče na njegov položaj. Čini se da bi kompanija u ovakvim situacijama mogla da unapredi svoj algoritam detekcije ovakvih upita i da odbije davanje odgovora na njih, kako bi se omogućila zaštita osetljivih podataka.

Primetno je da četbotovi ne informišu korisnike o automatizovanom donošenju pojedinačnih odluka. To je u suprotnosti sa čl. 13 GDPR-a koji predviđa da rukovalac (obrađivač) mora obavestiti korisnike o postojanju automatskih sistema.[25]

Odredbe ZZPL-a[26] su slične GDPR-u, a od posebnog značaja je činjenica da se Zakon ne primenjuje na podatke koji su dostupni svakome i koji su objavljeni u javnim glasilima, kao i na podatke koje je neko lice, sposobno da se stara o sebi, samo o sebi negde objavilo.[27] ZZPL takođe u čl. 4, tač. 13 štiti pojedince od povreda

[24] Ovde se takođe nameće pomenuto rešenje time što bi kompanija dala mogućnost korisnicima da isključe opciju prilikom kreiranja naloga. Neki autori takođe ukazuju na surovu realnost kršenja prava na informisanje i davanje pristanka korisnika još u najranijoj fazi istraživanja četbotova (Xiongbiao, 2024, p. 4). Izvesno je da se takvom praksom negira sama priroda pristanka za obradu ličnih podataka za koji se može reći da je jednostrani, kauzalni, dobročini ili teretni, neformalni, *inter vivos* i komutativni pravni posao kojim davalac pristanka daje ovlašćenje rukovaocu ili obrađivaču da mogu obrađivati određene vrste njegovih podataka u tačno određene svrhe (Andonović, 2024, p. 109).

[25] Međutim, obrađivač nije u obavezi da obavesti lice o pravu da ne bude podvrgnuto automatskom donošenju odluka. Čini se da je ovo još jedna mogućnost za *ChatGPT* da potencijalno ugrozi podatke korisnika, te je u tom smislu potrebno veće balansiranje.

[26] Naše pozitivno pravo preuzima osnovna načela zaštite podataka kao i samu definiciju ličnih podataka. Interesantno je da je prvobitan Model zakona o zaštiti podataka o ličnosti iz 2006. godine, imao sličnu definiciju, ali je imao dodatak kojim se tražilo da je „identitet određen ili se bez znatnog utroška vremena ili sredstava može odrediti" (Gajin, Resanović & Vodinelić, 2026, čl. 3, st. 1).

[27] Iz ove odredbe jasno je da je zakon nemoguće primeniti na zaštitu korisnika društvenih

ličnih podataka, kao i u slučajevima nezakonitog uništenja, gubitka, izmene ili neovlašćenog otkrivanja.[28]

Često se zaboravlja da podaci o ličnosti uživaju više nivoa zaštite. Tu obuhvatamo ustavnopravnu, upravnu, građanskopravnu i krivičnopravnu zaštitu (Đukić, 2017, p. 51). Kako ističe Kovačević (2023, p. 303), zaštita ličnih podataka često ima i širi okvir, koji prevazilazi privatnost, a koji uključuje pravičnost, transparentnost, odgovornost, nediskriminaciju, zakonitost i proporcionalnost, kao i proceduralnu prirodu.

Edukacija i informisanost korisnika o svim nivoima zaštite svakako bi doprinela manjim rizicima, ali bi takođe povećala opreznost i usklađenost *ChatGPT*-a u pružanju svojih usluga.

7. Zaključak

Imajući u vidu prethodno navedeno, potrebno je utvrditi na koji način se može postići veća zaštita podataka o ličnosti prilikom korišćenja četbotova. *ChatGPT* treba da radi na većem nivou usklađenosti, kako u fazi treninga sistema, tako i u fazi komunikacije sa korisnicima. Prvi korak u tom pravcu je i nedavno usvojen AI Act, a u vezi sa kojim je *ChatGPT* već napravio plan usklađenosti i vremenske okvire usvajanja.

Preporuke za kompaniju OpenAI, koja stoji iza *ChatGPT*-a, jasne su. Potreban je rad na uspostavljanju sistema koji će biti u skladu sa načelom minimizacije, omogućavajući prikupljanje samo onih podataka koji su neophodni. Osim toga, OpenAI bi trebalo da razmišlja u pravcu implementacije anonimizacije podataka pre njihovog skladištenja. Istovremeno, korisnici moraju biti obavešteni koji podaci se prikupljaju i kako mogu da ostvare svoja prava, te ostvarivanje tih prava mora biti olakšano u praksi. Takođe bi trebalo da kompanija poveća transparentnost u pogledu treninga, kao i da informiše javnost na koji način se smanjuje upotreba ličnih podataka u procesu treninga pre nego što se te informacije iskoriste u obuci modela.

mreža prilikom zloupotrebe objavljenih ličnih podataka od strane nekog trećeg lica. Međutim, obrada podataka nije dozvoljena kada fizičko lice nije dalo pristanak za obradu podataka, kada se obrada podataka vrši bez zakonskog ovlašćenja, kada je način obrade nedozvoljen ili kada nije jasna svrha obrade (Vilić & Radenković, 2015, p. 334).

[28] U ovakvim situacijama je neophodno da poverenik bude obavešten zajedno sa pogođenim pojedincima u slučaju postojanja visokog rizika. Kazna predviđena za kršenja prava u ovom slučaju dostiže maksimum od dva miliona dinara (ZZPL, čl. 95). U ovom slučaju poverenik bi bio ujedno i nadležan da pokrene postupak, te je pitanje kako bi se takav postupak završio i da li bi bilo kažnjavanja (Diligenski & Žižić, 2020, p. 141) ukoliko postoji povreda od strane četbota.

ChatGPT i OpenAI treba da dokažu da imaju stabilan bezbednosni sistem i tehničke mogućnosti da spreče povredu podataka o ličnosti. Ukoliko ipak dođe do povrede, kompanija mora imati mehanizme za otklanjanje štetnih posledica. Svaka povreda mora biti prijavljena nadležnom organu za zaštitu podataka u roku od 72 sata, a u skladu sa čl. 33 GDPR-a. Kako bi se osiguralo da se *ChatGPT* pridržava bezbednosnih mera, potrebno je pooštriti propise kojima bi se regulisalo puštanje u promet celog sistema. Povećanjem nivoa usklađenosti porasli bi ugled sistema i poverenje korisnika u ceo sistem, što treba da bude i cilj same kompanije. S druge strane, potrebno je povećati edukaciju korisnika i uputiti ih na pravilno i bezbedno korišćenje *ChatGPT*-a.

Konstantan razvoj novih tehnologija dovodi do česte izmene pravnih propisa pa su na subjektima odgovornost i obaveza da prate pravne akte koji se tiču oblasti veštačke inteligencije i da balansiraju između inovacija i zaštite podataka.

Usklađivanje sa propisima GDPR-a je složen proces jer je tanka linija koja deli usklađenost od mogućih povreda ličnih podataka. Poznavanje propisa nije samo obaveza korporacija koje razvijaju četbot sisteme već i obaveza pojedinaca koji koriste usluge takvih sistema. Svaki korisnik mora nastojati da unapredi svoje znanje u oblasti zaštite podataka i da bude svestan sankcija u slučaju nepridržavanja propisa.

Edukacija je najbolji vid prevencije te redovna obuka garantuje poznavanje važećih propisa u oblasti zaštite podataka o ličnosti. Kombinovanjem ovih metoda prevencije može se očekivati svojevrstan nivo pravne sigurnosti u ovoj oblasti.

Literatura

Alkaissi, H. & McFarlane, I. 2023. Artificial Hallucinations in ChatGPT: Implications in Scientific Writing. *Cureus*, 15(2), pp. 1-4. https://doi.org/10.7759/cureus.35179

Andonović, S. 2024. Institut pristanka kod zaštite ličnih podataka. U: Stanić, M. & Rajić Ćalić, J. (ur.), *Neobjavljeni radovi dr Stefana Andonovića.* Beograd: Institut za uporedno pravo, pp. 103-112.

Andonović, S. 2020. Normativni aspekti veštačke inteligencije u radu organa uprave u Republici Srbiji. U: Soković, S. (ur.), *Usklađivanje pravnog sistema Srbije sa standardima Evropske unije*: *zbornik radova*. Kragujevac: Pravni fakultet Univerziteta u Kragujevcu, pp. 141-154.

Andonović, S. 2019. *Zaštita podataka u elektronskoj javnoj upravi u Republici Srbiji – pravni aspekti.* Doktorska disertacija. Beograd: Pravni fakultet Univerziteta u Beogradu.

Avramović, D. & Jovanov, I. 2023. Sudijska (ne)pristrasnost i veštačka inteligencija. *Strani pravni život,* 67(2), pp. 161-177. https://doi.org/10.56461/SPZ_23201KJ

Cecconi, F. 2023. *AI in the Financial Markets: New Algorithms and Solutions*. Switzerland: Springer. https://doi.org/10.1007/978-3-031-26518-1

Choudhury, A. & Shamszare, H. 2023. Investigating the Impact of User Trust on Adoption and Use of ChatGPT: A Survey Analysis, *Journal of Medical Internet Research*, 25, pp. 1-11. https://doi.org/10.2196/47184

Diligenski, A. & Žižić, M. 2020. Pravo na naknadu štete kod povreda zaštite podataka o ličnosti. U: Andonović, S., Prlja, D. & Diligenski, A. (ur.), *Zaštita podataka o ličnosti u Srbiji: zbornik radova*. Beograd: Institut za uporedno pravo, pp. 139-151.

Đukić, D. 2017. Zaštita podataka o ličnosti sa osvrtom na novo zakonodavstvo Evropske unije u ovoj oblasti. *Pravni zapisi*, 7(1), pp. 49-60.

Gasmi, G. & Prlja, D. 2021. Ugrožavanje ljudskih prava i veštačka inteligencija. U: Perović Vujačić, J. S. (ur.), *Primena prava i pravna sigurnost: zbornik radova*. Zbornik radova Kopaoničke škole prirodnog prava Slobodan Perović, 3, pp. 323-335.

Gajin, S., Resanović, A. & Vodinelić, V. 2006. Model zakona o zaštiti podataka o ličnosti. *Hereticus – Časopis za preispitivanje prošlosti*, 4(3/4), pp. 138-156

Goldsteen, A., Ezov, G., Shmelkin, R., Moffie, M. & Farkash, A. 2022. Data Minimization for GDPR Compliance in Machine Learning Models. *AI Ethics*, 2, pp. 477-491. https://doi.org/10.1007/s43681-021-00095-8

Hasal, M., Nowaková, J., Saghair, K. A., Abdulla, H., Snášel, V. & Ogiela, L. 2021. Chatbots: Security, Privacy, Data Protection, and Social Aspects. *Wiley*, pp. 1-13. https://doi.org/10.1002/cpe.6426

Kovačević, T. 2023. Izazovi digitalizacije rada i zaštite ličnih podataka. *Strani pravni život,* 67(2), pp. 299-320. https://doi.org/10.56461/SPZ_23207KJ

Mathis, K. & Tor, A. 2022. *Law and Economics of the Digital Transformation*. Switzerland: Springer. https://doi.org/10.1007/978-3-031-25059-0

Milić, D. 2020. Legitimni interes kao osnov za obradu podataka o ličnosti. U: Andonović, S., Prlja, D. & Diligenski, A. (ur.), *Zaštita podataka o ličnosti u Srbiji: zbornik radova*. Beograd: Institut za uporedno pravo, pp. 47-60.

Naghiyev, K. 2024. ChatGPT from a Data Protection Perspective. *Baku State University Law Review*. 10(1) pp. 1-34. https://doi.org/10.2139/ssrn.4818860

Savar, M. P. 2023. ChatGPT: A Study of AI Language Processing and its Implications. *International Journal of Research Publication and Reviews*, 4(2), pp. 435-440. https://doi.org/10.55248/gengpi.2023.4218

Sebastian, G. 2023. Privacy and Data Protection in ChatGPT and Other AI Chatbots: Strategies for Securing User Information. *International Journal of Security and Privacy in Pervasive Computing*, 15(1), pp. 1-14. https://doi.org/10.4018/IJSPPC.325475

Sen, Z., Uygun, O. & Erden, C. 2023. *Advances in Intelligent Manufacturing and Service System Informatics*. Singapore: Springer. https://doi.org/10.1007/978-981-99-6062-0

Tošić, I. & Novaković, O. 2020. Uticaj nove regulacije u oblasti zaštite podataka o ličnosti na rad osiguravajućih društava. U: Andonović, S., Prlja, D. & Diligenski, A. (ur.), *Zaštita podataka o ličnosti u Srbiji: zbornik radova*. Beograd: Institut za uporedno pravo, pp. 93-103.

Vilić, V. & Radenković, I. 2015. Pravo na privatnost u svetlu zakona o zaštiti podataka o ličnosti. *Pravni život*, 64(10), pp. 331-341.

Villaronga, E., Kieseberg, P. & Li, T. 2018. Humans Forget, Machines Remember: Artificial Intelligence and the Right to be Forgotten. *Computer Law & Security Review*, 34(2), pp. 304-313. https://doi.org/10.1016/j.clsr.2017.08.007

Zarifis, A., Ktoridou, D., Efthymiou, L. & Cheng, X. 2024. *Business Digital Transformation*. Switzerland: Palgrave Macmillan. https://doi.org/10.1007/978-3-031-33665-2

Xiongbiao, Y., Yan, Y., Li, J. & Jiang, B. 2024. Privacy and Personal Data Risk Governance for Generative Artificial Intelligence: A Chinese Perspective. *Telecommunications Policy*, 48, pp. 1-14. https://doi.org/10.1016/j.telpol.2024.102851

Pravni izvori

Artificial Intelligence Act (AI Act) 2024. *Official Journal of the European Union*, L 1689. Dostupno na: https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng (20. 5. 2025).

California Consumer Privacy Act 2018. Dostupno na: https://govt.westlaw.com/calregs/Document/IB2273E40D44D11ED85F08DB10BE8 E2E0 (20. 4. 2025).

General Data Protection Regulation (GDPR) 2016. *Official Journal of the European Union*, L 119, 2016/679. Dostupno na: https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng (20. 5. 2025).

Krivični zakonik RS. *Službeni glasnik RS*, br. 85/2005, 88/2005 – ispr., 107/2005 – ispr., 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016, 35/2019, 94/2024.

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

Zakon o obligacionim odnosima. *Službeni list SFRJ*, br. 29/1978, 39/1985, 45/1989 – odluka USJ i 57/1989, *Službeni list SRJ*, br. 31/1993; *Službeni list SCG*, br. 1/2003 – Ustavna povelja; *Službeni glasnik RS*, br. 18/2020.

Internet izvori

A Primer on the EU AI Act. 2024. Dostupno na: https://openai.com/global-affairs/a-primer-on-the-eu-ai-act/, 17. 1. 2025.

Data Controls FAQ. 2024. Dostupno na: https://help.openai.com/en/articles/7730893-data-controls-faq, 17. 1. 2025.

How to Delete Your Account. Dostupno na: https://help.openai.com/en/articles/6378407-how-to-delete-your-account, 17. 1. 2025.

Imran Rahman-Jones. ChatGPT: Italy Says OpenAI's Chatbot Breaches Data Protection Rules. 2024. Dostupno na: https://www.bbc.com/news/technology-68128396, 11. 1. 2025.

March 20 ChatGPT Outage: Here's What Happened. 2023. Dostupno na: https://openai.com/index/march-20-chatgpt-outage/, 16. 1. 2025.

Privacy Policy. 2024. Dostupno na: https://openai.com/policies/row-privacy-policy/ (17. 1. 2025). Security & Privacy. Dostupno na: https://openai.com/security-and-privacy/, 17. 1. 2025.

Vlada Republike Srbije. 2020. Etičke smernice za razvoj, primenu i upotrebu pouzdane i odgovorne veštačke inteligencije. Dostupno na: https://www.ai.gov.rs/tekst/sr/586/eticke-smernice.php, 5. 1. 2025.

Vlada Republike Srbije. 2019. Strategija razvoja veštačke inteligencije u Republici Srbiji za period 2020–2025. Dostupno na: https://www.srbija.gov.rs/extfile/sr/437304/strategija_razvoja_vestacke_inteligencije261219_2_cyr.pdf, 17. 1. 2025.

Vlada Republike Srbije. 2019. Strategija razvoja veštačke inteligencije u Republici Srbiji za period 2020–2025. Dostupno na: https://www.srbija.gov.rs/tekst/437277, 2. 2. 2025.

Wim Nauwelaerts. Dutch Data Protection Authority Warns That Using AI Chatbots Can Lead to Personal Data Breaches. Dostupno na: https://www.alstonprivacy.com/dutch-data-protection-authority-warns-that-using-ai-chatbots-can-lead-to-personal-data-breaches/, 11. 1. 2025.