

DOI: 10.46793/GlasnikDN16.2.068C

Originalni naučni članak

UDK broj

342.738

004.8:17

**Nenad Cvjetičanin, doktorand\***

Pravni Fakultet Univerziteta Union, Beograd, Republika Srbija

Union University, Law School, Belgrade, Republic of Serbia

**Primljen:** 14. oktobra 2024. godine

**Vraćen na doradu:** 27. oktobra 2024. godine

**Prihvaćen:** 12. novembra 2024. godine

## UTICAJ VEŠTAČKE INTELIGENCIJE NA ZAŠTITU PODATAKA O LIČNOSTI

### **Apstrakt**

*Tehnologije veštačke inteligencije (VI) ubrzano napreduju, oslanjajući se na velike količine podataka kako bi se razvijale i pružale inovativne usluge. VI je našla primenu u praktično svim sektorima privrede, kao i u svakodnevnom životu, a gorivo na kome zasniva svoj rast je eksploatacija podataka. Među tim podacima, najbitnije mesto zauzimaju podaci o ličnosti, čija obrada mora biti u skladu sa Zakonom o zaštiti podataka o ličnosti, odnosno sa Opštom Uredbom o zaštiti podataka o ličnosti (GDPR). Donošenjem Uredbe o veštačkoj inteligenciji, koja je stupila na snagu 1. avgusta 2024. godine, postavljeni su novi regulatorni okviri za razvoj i upotrebu sistema veštačke inteligencije u Evropskoj uniji. Iako su ovi zakoni specifični za različite aspekte obrade podataka, njihova primena u kontekstu veštačke inteligencije neizbežno se prepliće, postavljajući pravne*

---

\* E-mail adresa: [nenad.cvjeticanin@cvjeticaninlegal.com](mailto:nenad.cvjeticanin@cvjeticaninlegal.com), ORCID ID: <https://orcid.org/0009-0008-1913-876X>.

*izazove za pružaoce i korisnike sistema VI. Kada su u pitanju podaci o ličnosti, Opšta uredba o zaštiti podataka o ličnosti (GDPR), predstavlja akt najviše pravne snage u Evropskoj uniji. Međutim, da bi se obezbedila usklađenost (eng. “compliance”), prilikom stavljanja u upotrebu sistema veštačke inteligencije važno je primeniti oba propisa.*

**Ključne reči:** *veštačka inteligencija, zaštita podataka o ličnosti, GDPR, automatizovana obrada podataka, minimizacija obrade podataka, transparentnost*

**JEL klasifikacija:** K10, K36, L80, O33

## **Uvod**

Predmet ovog rada jeste uticaj sistema veštačke inteligencije na zaštitu podataka o ličnosti. Posebno će se analizirati koristi, ali i neminovni štetni uticaji i posledice koje društvo može imati. Analiza će obuhvatiti odnos Uredbe o veštačkoj inteligenciji prema zaštiti podataka o ličnosti, kao i odnos te Uredbe sa **GDPR**-om i našim Zakonom o zaštiti podataka o ličnosti.

Članak koristi kombinaciju pravno-dogmatske, komparativne i interdisciplinarnе metodologije (obuhvatajući etičke i tehnološke aspekte), kako bi se pružila sveobuhvatna analiza uticaja **VI** na zaštitu podataka o ličnosti.

Plan razvoja veštačke inteligencije u Srbiji je regulisan neobavezujućim dokumentom – Strategijom za razvoj veštačke inteligencije za period od 2020–2025. Iako još nije istekao rok primene prve strategije, bez završnog izveštaja o ostvarenim ciljevima, pomalo iznenada, u javnoj raspravi se tokom juna 2024. godine našla nova Strategija za novi petogodišnji period od 2024–2030. godine.

Regulatorni okviri koji se odnose na etičke i pravne aspekte primene **VI** moraju postići odgovarajući balans između zaštite građana i podsticanja inovacija. Iako razvoj **VI** donosi mnogobrojne prednosti, istovremeno postavlja i značajne izazove, kako na

individualnom, tako i na društvenom nivou. Kao što je istaknuto u još uvek važećoj Strategiji, kako bi se osigurala dostupnost, bezbednost i ravnomerna primena **VI**, te izgradilo poverenje društva prema ovoj tehnologiji, neophodno je da se tehnološki napredak prati odgovornim promišljanjem i pravovremenim rešavanjem izazova koji prate razvoj i implementaciju **VI**. Strategija identifikuje nekoliko ključnih zahteva, među kojima su: ljudska intervencija i nadzor, tehnička robustnost i sigurnost, zaštita privatnosti i upravljanje podacima, transparentnost, raznolikost, pravednost i nediskriminacija, dobrobit za društvo i zaštita životne sredine, kao i odgovornost. Takođe, otvoreni podaci predstavljaju neophodan resurs za dalji razvoj veštačke inteligencije.

Algoritmi veštačke inteligencije se masovno primenjuju radi povećanja efikasnosti mnogih poslovnih modela, kao i u „blockchain“ tehnologijama.

Korišćenje „blockchain“ platforme takođe omogućava unapređeno donošenje odluka zasnovanih na podacima, zahvaljujući integraciji sa analitičkim alatima i alatima veštačke inteligencije. Ovo omogućava kompanijama ne samo da reaguju na trenutne trendove, već i da predviđaju buduće promene u preferencijama potrošača i uslovima na tržištu. [8, str. 55-95].

Kako bi se unapredile tehnologije veštačke inteligencije i mašinskog učenja, potrebna je velika količina podataka, koja može uključivati i podatke o ličnosti. Uredba o veštačkoj inteligenciji, stupivši na snagu 1. avgusta 2024. godine, uvodi u Evropsko pravo obavezujući okvir za razvoj i upotrebu sistema **VI**. Međutim, kada su u pitanju podaci o ličnosti, još uvek je neophodno usklađivanje sa Opštom uredbom o zaštiti podataka (**GDPR**).

Kreatori Uredbe pokušali su da pronađu balans između primene veštačke inteligencije u svakodnevnom životu i zaštite bezbednosti i ljudskih prava putem pristupa koji se zasniva na rizicima (risk-based approach), te se može razlikovati primena veštačke inteligencije koja predstavlja neprihvatljiv rizik, visok rizik i nizak ili minimalan rizik. Reč je, zapravo, o horizontalnom regulatornom okviru prema kojem

se kreiranje, uvođenje na tržište i primena sistema veštačke inteligencije određuje na osnovu rizika koji takvi sistemi predstavljaju za bezbednost i zdravlje ljudi i osnovna prava. Tako je primena veštačke inteligencije koja predstavlja neprihvatljiv rizik zabranjena, osim u izuzetnim slučajevima. U Aneksu III Predloga uredbe su navedene oblasti u kojima primena veštačke inteligencije predstavlja visok rizik. To su, na primer, primena sistema veštačke inteligencije prilikom ocenjivanja učenika/studenta, procenjivanja kreditne sposobnosti, ocenjivanja prilikom zasnivanja radnog odnosa, sistemi za nadzor (sistemi za prepoznavanje lica), prilikom utvrđivanja verodostojnosti putničkih dokumenata (migracije, azil i kontrola granica), prilikom primene prava na određene činjenice (pravosuđe i demokratski procesi) [7, str. 1-11].

Uredba koja sadrži odredbe i o etičkim standardima je naišla na široko odobravanje, te se smatra da ima potencijal da postane lider u oblasti pravne regulative veštačke inteligencije na globalnom nivou, odnosno da postane tzv. “superregulator” [1, str.1]. Naglasak bi, međutim, prema jednom mišljenju, trebalo staviti na činjenicu da je intencija Evropske unije da jasno zaštiti vladavinu prava od “vladavine tehnologije” [1, str.1]. Namera je da ovaj pravni okvir sadrži harmonizovana pravila koja su i u saglasnosti sa postojećim instrumentima zaštite ljudskih prava u Evropskoj uniji i pravnom regulativom EU koja se odnosi na zaštitu podataka, zaštitu potrošača, zabranu diskriminacije i rodnu ravnopravnost [11, str. 2-6].

Sa druge strane, u maju mesecu 2024. godine je oformljena radna grupa za donošenje srpskog, odnosno domaćeg Zakona o veštačkoj inteligenciji, koja je najavila da će nacrt teksta zakona biti pripremljen i stavljen na javnu raspravu u roku od godinu dana. Za očekivati je da će tekst našeg zakona biti u velikom procentu usklađen sa Uredbom o veštačkoj inteligenciji, zbog obaveza koji je Srbija preuzela po Sporazumu o stabilizaciji i pridruživanju.

## **1. Rizici**

Hraneći se privatnim podacima, algoritmi se pojavljuju kao novi subjekti moći kojima nedostaje transparentnost, a vrlo često i objektivnost. Njihov uticaj je prisutan u svim sferama društva, jer se koriste ne samo za funkcionisanje društvenih mreža i drugih platformi, već i u bezbednosnim, finansijskim, zdravstvenim i drugim institucijama [4, str. 41]. Oni su problematični upravo zbog toga što nisu ni objektivni ni neutralni, već su veoma često pristrasni i skloni diskriminatornim praksama [3, str. 298-316; 2, str. 1]. Međutim, ključni argument koji osporava etičnost algoritamske kulture je taj da su algoritmi „tajni” mehanizmi koji na netransparentan način tumače i oblikuju podatke, a zatim na osnovu tih tumačenja donose određene odluke [4, str. 41].

Jedan od izazova su i društveni i organizacioni stavovi prema tehnologiji [12, str. 339]. Dalje, **VI** može narušiti privatnost i slobodu građana, naročito kada je u pitanju javna bezbednost. Organizacije poput policije i avio-kompanija mogu prikupljati osetljive podatke građana. Građani svakodnevno ustupaju kontrolu nad privatnim informacijama. Vlade mogu koristiti te informacije u najrazličitije svrhe. Kada je reč o privatnosti, postoji velika i opravdana zabrinutost u pogledu ovog izazova. **VI** prikuplja ogromne količine informacija, uključujući i podatke sa mobilnih uređaja i druge elektronike, i ekstrapolira ih, tako da profesionalci mogu donositi odluke zasnovane na tim podacima. Ugrožavanje privatnosti predstavlja, dakle, prvi izazov. Povećana upotreba automatizovanih sistema i veštačke inteligencije izlaže klijente riziku gubitka privatnosti. Kompanije su u mogućnosti da uporede kupovno ponašanje svojih kupaca, zbog čega su kupci u opasnosti da pronađu ove informacije u javnom domenu ili da budu „prodani“ drugim zainteresovanim stranama. Takođe, prodavci mogu otkriti da su njihovi prethodno personalizovani podaci koji čine osnovu njihovih odnosa sa kupcima sada lako dostupni drugim delovima kompanije, smanjujući njihovu efikasnost [6, str. 2].

## **2. Obuhvat Uredbe o veštačkoj inteligenciji i GDPR-a**

Uredba o veštačkoj inteligenciji reguliše razvoj, plasman, puštanje u upotrebu i korišćenje sistema **VI**, dok **GDPR** pokriva obradu podataka o ličnosti bez obzira na vrstu tehnologije korišćene u tom procesu. Kada sistemi **VI** koriste podatke o ličnosti za treniranje modela ili kada se ti podaci obrađuju tokom njihove upotrebe, obe uredbe postaju primenljive. Što se tiče ličnog obuhvata, Uredba o veštačkoj inteligenciji cilja pružaoce i korisnike sistema **VI**. U kontekstu **GDPR**-a, ti isti pružaoци i korisnici su rukovaoci i obrađivači podataka, odgovorni za poštovanje pravila o zakonitosti obrade.

Tačka sedamdeset jedan Preambule, kao i član dvadeset dva Opšte uredbe o zaštiti podataka o ličnosti EU direktno obuhvata algoritamsko donošenje odluka. U njoj se utvrđuje pravo pojedinca da zahteva da se na njega ne odnosi odluka doneta isključivo na osnovu automatizovane obrade podataka koja proizvodi pravne posledice za njega ili koja na njega značajno utiče. Navedeni su primeri odbijanja kredita putem interneta ili prakse zapošljavanja putem interneta. Ovakva automatizovana obrada podataka uključuje izradu profila, odnosno procenjivanje ličnih karakteristika pojedinca, posebno onih vezanih za rezultate na poslu, ekonomsko stanje, zdravlje, lične preferencije ili interese, pouzdanosti ili ponašanja, lokacije ili kretanja, kada ona proizvodi pravne posledice koje se odnose na pojedinca ili na njega utiču. Međutim, donošenje odluka koje se temelji na takvoj obradi, što uključuje i izradu profila, može biti dopušteno ako to dozvoljava pravo EU ili pravo države članice kojem podleže obrađivač podataka, između ostalog, u svrhe praćenja i sprečavanja prevare i poreske utaje, u skladu s propisima, standardima i preporukama institucija EU ili nacionalnih organa. Na na taj način se osigurava bezbednost i pouzdanost usluge koju pruža obrađivač podataka ili ako je neophodno za sklapanje ili izvršavanje ugovora između pojedinca i obrađivača ili kada je pojedinac izričito dao svoju saglasnost. [10, str. 15-47].

### **3. Primena oba pravila**

Obzirom na razliku u obuhvatu **GDPR**-a i Uredbe o veštačkoj inteligenciji, potrebno je odrediti koji propis se primenjuje u datoj situaciji kako bi se osigurala usklađenost. Kada podaci o ličnosti služe treniranju sistema **VI**, pružalac mora obezbediti da obrada bude u skladu sa oba pravila. Na primer, rukovalac podacima mora osigurati da su podaci korišćeni u skladu sa legitimnim pravnim osnovama definisanim u **GDPR**-u, kao i da je svrha njihove obrade jasno definisana. U nastavku je izneto nekoliko različitih scenaria i primera kumulativne primene Uredbe o **VI**, odnosno **GDPR**-a, kao i oni u kojima je primena isključiva, odnosno u kojima primene nema.

*Tabela 1. Primenljivost Uredbe o uredbe o VI u odnosu na GDPR*

Scenario	Primer	Da li je primenljiva Uredba o VI ili GDPR?
Podaci o ličnosti su potrebni za razvoj i/ili korišćenje sistema <b>VI</b>	Pružaoци zdravstvenih usluga koriste sistem <b>VI</b> za analizu medicinskih kartona pacijenata i preporuku terapija	Primenjuju se i Uredba o veštačkoj inteligenciji i <b>GDPR</b>
Podaci o ličnosti nisu potrebni za razvoj ni korišćenje sistema <b>VI</b>	Kompanija za logistiku koristi <b>VI</b> za optimizaciju upravljanja skladištem na osnovu podataka o proizvodima, bez obrade podataka o ličnosti	Primenjuje se samo Uredba o veštačkoj inteligenciji
Podaci o ličnosti se obrađuju za razvoj ili korišćenje sistema <b>VI</b> koji nije predmet Uredbe o veštačkoj inteligenciji	Univerzitetski istraživač obrađuje podatke studenata za akademska istraživanja bez komercijalne svrhe	Primenjuje se samo <b>GDPR</b>

Podaci o ličnosti nisu potrebni za razvoj ili korišćenje VI sistema koji nije predmet Uredbe o veštačkoj inteligenciji	Sistem VI se koristi u odbrambenoj industriji za obradu geolokacije terena	Nisu primenljivi ni Uredba o veštačkoj inteligenciji ni <b>GDPR</b>
--	--	---

*Izvor: autor*

#### **4. Pomirenje načela minimizacije sa potrebom za masovnom obradom podataka**

Sistemi VI, naročito oni zasnovani na mašinskom učenju, često zahtevaju velike količine podataka za treniranje. Međutim, čl. 5. Zakona o zaštiti podataka o ličnosti propisuje načelo minimizacije, što znači da rukovalac mora osigurati da se koristi samo onoliko podataka koliko je neophodno za postizanje određene svrhe.

Na primer, za razvoj sistema VI koji se koristi za analizu specifične bolesti, nije potrebno koristiti podatke o celoj populaciji, već samo o onoj koja je obolela od date bolesti. Ukoliko je moguće, preporučuje se korišćenje pseudonimizovanih baza podataka, kako bi se smanjila mogućnost zloupotrebe podataka o ličnosti.

**GDPR** u članu 25. st. 1. ukazuje na potrebu pseudonimizacije u kontekstu tehnološkog razvoja što VI tehnologije svakako jesu. Rukovalac, uzimajući u obzir najnovija tehnološka dostignuća, troškove sprovođenja, kao i prirodu, obim, kontekst i svrhu obrade, te rizike za prava i slobode fizičkih lica, primenjuje odgovarajuće tehničke i organizacione mere, kao što je pseudonimizacija. Te mere su osmišljene radi efikasnog sprovođenja načela zaštite podataka, uključujući i minimizaciju obrade, i obezbeđuju zaštitu prava lica na koja se podaci odnose, u skladu sa zahtevima ove uredbe.

Član 10. Uredbe o veštačkoj inteligenciji spominje pseudonimizaciju u odeljku koji se odnosi na visokorizične sisteme VI i obradu posebne kategorije podataka o ličnosti. Dobavljači visokorizičnih sistema veštačke inteligencije mogu izuzetno obrađivati posebne kategorije podataka o ličnosti radi otkrivanja i



ispravljanja pristrasnosti, pod uslovom da ne postoji drugi delotvoran način za postizanje tog cilja, te da se obrada sprovodi uz tehnička ograničenja ponovne upotrebe podataka i primenu najsavremenijih mera sigurnosti, uključujući pseudonimizaciju. Ova obrada mora biti u skladu sa relevantnim propisima, **GDPR**-om, Policijskom direktivom i drugim merodavnim dokumentima.

### **5. Pravo na informisanost lica čiji se podaci obrađuju (transparentnost sistema VI)**

Tajnost rada algoritama objašnjava se, sa jedne strane, tehničkim osobinama algoritama koji su zapravo veoma kompleksni sistemi, a, sa druge, time što je diskrecija neophodna kako bi se kompanija koja ih koristi zaštitila; na primer, kompanija Facebook štiti tajnu funkcionisanja algoritama zato što bi u suprotnom moglo doći do zloupotreba [4, str. 41]. Kritike na račun rada algoritama usmerene su, dakle, na to što su algoritmi po prirodi potpuno neprozračne „crne kutije”, pa je samim tim njihova moć da donose odluke problematična [9, str. 568-571].

Nadzor, dakle, sa pojavom ovih novih informacionih tehnologija i internet medija postaje algoritamski, neproziran i tajan. On je povezan sa jednim potpuno novim oblikom kontrole koja više nije vezana za ljudski faktor, već za veštačku inteligenciju koja na netransparentan način koristi privatne podatke. Pokušaji da se algoritamska obrada podataka ograniči tako da se zaštite ljudska prava i slobode ostaju nedovršeni. Jedan od mehanizama za zaštitu prava na privatnost u pogledu algoritamske obrade podataka predstavlja Opšta uredba Evropske unije o zaštiti podataka o ličnosti, međutim, on je problematičan upravo zbog toga što algoritmi imaju osobine crne kutije, pa je samim tim tehnički previše zahtevno da se uopšte omogući princip transparentnosti definisan u ovom pravnom dokumentu [5, str. 19-47].

Uredba o veštačkoj inteligenciji u recitalu 27. govori o transparentnosti sistema **VI**, ukazujući u tom pogledu na shodnu primenu **GDPR**-a i Policijske direktive prilikom obrade podataka o

ličnosti. Transparentnost podrazumeva da se sistemi veštačke inteligencije razvijaju i koriste na način koji omogućava odgovarajuću sledljivost i objašnjivost, uz istovremeno informisanje lica o tome da komuniciraju ili su u interakciji sa sistemom veštačke inteligencije, kao i propisno informisanje subjekata koji uvode takav sistem o njegovim sposobnostima i ograničenjima. Takođe, lica na koja sistem veštačke inteligencije utiče moraju biti obaveštena o svojim pravima. Iako su sistemi **VI** često složeni i neprozirni, **GDPR** zahteva od rukovalaca da lica čiji se podaci obrađuju budu jasno i precizno informisana o svim aspektima obrade. To uključuje informisanje o načinu rada sistema **VI** i njegovom potencijalnom uticaju na prava i slobode pojedinaca. Primera radi, ukoliko sistem automatski donosi odluke koje imaju pravne posledice po pojedince, rukovalac je dužan da pruži dovoljno informacija o sistemu koji stoji iza tih odluka i o posledicama obrade.

### **Zaključak**

Razvoj i primena veštačke inteligencije nužno zavise od korišćenja velikih količina podataka, što stvara izazov u usklađivanju sa važećim propisima o zaštiti podataka o ličnosti. Primena oba zakona — Zakona o veštačkoj inteligenciji i **GDPR**-a — zahteva pažljivu procenu svrhe i obima obrade podataka o ličnosti, kao i postizanje ravnoteže između potrebe za korišćenjem velikih baza podataka o ličnosti i načela minimizacije njihove upotrebe. Osiguranje transparentnosti i pružanje adekvatnih informacija licima čiji se podaci obrađuju ključni su koraci u ostvarivanju zakonite obrade. Radi pomirenja ove dve krajnosti neophodno bi bilo pronaći fini balans kako bi se osigurala zaštita podataka o ličnosti, sa jedne strane, kao i nesmetan razvoj naprednih tehnologija, sa druge strane.

### **Bibliografija:**

1. Biber, Dr Sümeyye Elif, „Machines Learning the Rule of Law: EU Proposes the World’s first Artificial Intelligence Act“, *VerfBlog*, 2021, 1.
  2. Borgesius, Frederik J. Zuiderveen, “Strengthening legal protection against discrimination by algorithms and artificial intelligence”, *The International Journal of Human Rights*, 2020, 1.
  3. Browning, Matthew, Arrigo A. Bruce, “Stop and Risk: Policing, Data, and the Digital Age of Discrimination”, *American Journal of Criminal Justice*, 2020, 298-316.
  4. Bucher, Taina, „If... Then: Algorithmic Power and Politics“, Oxford: Oxford University Press, 2018, 41.
  5. Crockett Keeley, O’Shea, Krügel Tina, Khan Wasiq, “Reconciling Adapted Psychological Profiling with the new European Data Protection Legislation”, *Computational Intelligence*, vol 893. Springer, 2021, 19-47.
  6. Dwivedi K. Yogesh, Hughes Laurie, Elvira Ismagilova et al, „Artificial Intelligence (AI): Multidisciplinary Perspectives on Emerging Challenges, Opportunities, and Agenda for Research, Practice and Policy“, *International Journal of Information Management*, vol. 57, 2021, 2.
  7. Kop Mauritz, „EU Artificial Intelligence Act: The European Approach to AI“, *Stanford - Vienna Transatlantic Technology Law Forum, Transatlantic Antitrust and IPR Developments*, Stanford University, Issue No. 2/2021, 1-11.
  8. Nikivorov Aleksei, „Exploring blockchain technology and its impact in e-commerce“, Vol. 16 No. XVI: *Journal of Social Sciences [Glasnik za društvene nauke]*, 2024, 55-95.
  9. Pasquale, F, „The Black Box Society: The Secret Algorithms That Control Money and Information“, Cambridge Massachussets: Harvard University Press, 2015, 568-571.
  10. Prlja Dragan, Gasmi Gordana, & Korać Vanja, *Ljudska prava i veštačka inteligencija*, Institut za uporedno pravo, 2022, 15-47.
-

11. Townsend Bev, „Decoding the Proposed European Union Artificial Intelligence Act“, American Society of International Law, ASIL Insights, Volume: 25 Issue: 20, 2021, 2-6.
12. Vasiljeva Tatjana, Kreituss Ilmars, Lulle Ilze, „Artificial Intelligence: The Attitude of the Public and Representatives of Various Industries“, Journal of Risk and Financial Management 14(8): 2021, 339

---

**Pravni izvori:**

13. Ustav RS („Sl. glasnik RS“, br. 98/2006 i 115/2021).
14. Zakon o zaštiti podataka o ličnosti („Sl. glasnik RS“, br. 87/2018).
15. Uredba (EU) 2016/679 Evropskog Parlamenta i Saveta od 27. aprila 2016. o zaštiti fizičkih lica u odnosu na obradu podataka o ličnosti, i o slobodnom kretanju takvih podataka i o stavljanju Direktive 95/46/EZ van snage (Opšta uredba o zaštiti podataka).
16. Uredba (EU) 2024/1689 Evropskog Parlamenta i Saveta od 13. juna 2024. o utvrđivanju usaglašenih pravila o veštačkoj inteligenciji i o izmeni uredbi (EZ) br. 300/2008, (EU) br. 167/2013, (EU) br. 168/2013, (EU) 2018/858, (EU) 2018/1139 i (EU) 2019/2144, kao i direktiva 2014/90/EU, (EU) 2016/797 i (EU) 2020/1828 (Zakon o veštačkoj inteligenciji).
17. Strategija razvoja razvoja veštačke inteligencije u Republici Srbiji za period 2020-2025. godina („Sl. Glasnik RS“, br. 96/2019).

## **THE IMPACT OF ARTIFICIAL INTELLIGENCE ON PERSONAL DATA PROTECTION**

### ***Abstract***

*Artificial intelligence (AI) technologies are rapidly advancing, relying on vast amounts of data in order to evolve and provide innovative services. AI has found applications in practically all sectors of the economy, as well as in everyday life, while the fuel driving its growth is the exploitation of various types of data. Among these, personal data holds the most significant position, and its processing must comply with the Personal Data Protection Act, as well as the General Data Protection Regulation (GDPR). With the adoption of the Artificial Intelligence Regulation, which came into effect on August 1, 2024, new regulatory frameworks have been established for the development and use of AI systems within the European Union. Although these laws are specific to different aspects of data processing, their application in the context of artificial intelligence inevitably overlaps, presenting legal challenges for both AI system providers and users. When it comes to personal data, the General Data Protection Regulation (GDPR) remains the highest legal authority in the European Union. However, to ensure compliance when deploying AI systems, it is important to apply both regulations.*

**Keywords:** *artificial intelligence, personal data protection, GDPR, automated data processing, data processing minimization, transparency.*

**JEL classification:** K10, K36, L80, O33