BE
RISK
PROTECTED.

AI I METAVERZUM.
ZAMKE I PREDNOSTI.
ETIKA I BEZBEDNOST.

SADRŽAJ

Fotografije: Pexels i Pixabay
Izdavač: **BeRiskProtected**

**preuzimanje sadržaja je dozvoljeno uz navođenje izvora sa linkom*

DA LI ĆE AI “UBITI PRASE”?!

Kad je svojevremeno Nikola Tesla otkrio potencijal naizmenične struje, suočio se sa žestokim otporom svog savremenika Tomasa Edisona, zagovornika jednosmerne struje. Legenda kaže da je Edison išao od grada do grada, nosio prase i demonstrirao od mesta do mesta kako Teslina struja može da ubije – naravno, puštajući je kroz siroto prase. Deo javnosti je time uplašio, ali je naizmenična struja ipak pobedila. Zato danas živimo u osvetljenim gradovima, snabdevamo se proizvodima i uslugama koje nam je omogućila struja, pa čak i internet koristimo upravo zahvaljujući ovom “opasnom” otkriću.

Reklo bi se da se na sličnom raskršću nalazimo i danas sa veštačkom inteligencijom.

Optimistički scenario već gledamo: AI podiže *produktivnost* - automatizuje rutinske zadatke, oslobađa

ljudski potencijal za kreativniji rad; otvara *nova tržišta* - od personalizovanog obrazovanja do autonomnih vozila i virtuelnih svetova; menja *zdravstvo* - ubrzava dijagnostiku, omogućava prediktivnu analizu i personalizovanu terapiju; uvodi revoluciju u *finansije* - donosi pametne algoritme za investiranje, zaštitu od prevara, inkluziju za one bez bankarskog pristupa.

Ali svaki napredak nosi i senku.

Pesimistički scenario donosi ozbiljne rizike: preti nezaposlenošću – zamenom ljudi u administraciji, transportu pa čak i kreativnim industrijama; uveliko se pojavljuju *deepfake prevare* - lažni video snimci i glasovne imitacije koje mogu ugroziti bezbednost i demokratiju; preti *gubitkom kontrole* - AI sistemi bez regulative mogu donositi odluke koje niko ne razume pa ne može ni zaustaviti.

I tu dolazimo do najvažnijeg pitanja: kako izgleda **"željeni" scenario**?

To je budućnost u kojoj veštačku inteligenciju ne odbacujemo zbog straha, ali je ni ne prihvatamo bezuslovno. U tom scenariju koristimo prednosti uz jasna pravila, etičke okvire I obrazovanu javnost. Baš kao što smo kroz regulaciju i infrastrukturu ukrotili struju, tako i AI treba da postane deo šireg društvenog dogovora.

Tehnologija sama po sebi nije ni dobra ni loša - sve zavisi od načina na koji je koristimo. Kombinacijom znanja i opreza, veštačka inteligencija može postati najvažniji alat našeg doba. Onaj koji, poput struje, menja svet iz korena — ali u pravcu koji sami izaberemo.

« POVRATAK NA SADRŽAJ

KAKO VEŠTAČKA INTELIGENCIJA MENJA POSLOVANJE

Piše:
Vladeta Radovanović,
CEO i osnivač **Presta**

AI sve češće zauzima centralnu poziciju kao ključni alat za unapređenje procesa i podizanje kvaliteta pruženih usluga. Stoga, ima sve važnije mesto u IT sektoru, jer donosi rešenja koja su do pre nekoliko godina delovala nezamislivo: od automatizacije rutinskih zadataka, preko pametne analize velikih količina podataka, pa sve do personalizovanih korisničkih iskustava. Uvođenjem ovih tehnologija, IT sektor postaje brži, precizniji i prilagodljiviji, što ne samo da unapređuje poslovanje, već i olakšava život krajnjim korisnicima.

PRIMER IZ PRAKSE

U konkretnom poslovnom scenariju sa kojim smo imali iskustva, jedna organizacija svakodnevno se suočavala sa velikim brojem dokumenata i stalnom potrebom za njihovom obradom. Proces je podrazumevao ručni pregled i unos podataka, što je bilo sporo, sklono greškama i zahtevno za ljudske resurse. Detaljna analiza procesa rada i precizno definisanje ključnih problema pokazali su da je neophodno pronaći konstruktivno rešenje koje će obezbediti bržu, tačniju i ekonomičniju obradu podataka.

Kao odgovor na identifikovane izazove, odlučeno je da se primeni AI u najkritičnijoj tački poslovanja, u fazi obrade dokumenata. Cilj implementacije bio je da se automatizuje proces koji je do tada bio pretežno manuelan, kako bi se povećali brzina, pouzdanost i tačnost rada. Primena AI omogućila je da se dokumenta automatski čitaju, dok se relevantni podaci prepoznaju i unose u odgovarajuće forme.

Rezultat ove primene vidljiv je kroz višestruko povećanje efikasnosti.

Vreme obrade dokumentacije smanjeno je sa nekoliko minuta na svega nekoliko sekundi po dokumentu, a potencijalne greške karakteristične za manuelni unos gotovo su u potpunosti eliminisane.

Primer iz prakse prikazuje kako dobro implementirana inteligencija, na ključnom mestu u poslovanju, može potpuno promeniti poslovanje, i manuelni, tradicionalni rad transformisati u automatizovan proces rada. To direktno utiče na buduće planiranje poslovanja, pogotovu kada se govori od profitabilnosti određenog sektora i daljem planiranju, odnosno preraspodeli budžeta.

TRI PRISTUPA PRIMENE AI REŠENJA

Pored praktične implementacije, važno je sagledati i nivo primene AI rešenja u odnosu na obim i potrebe organizacije. Postoje tri pristupa:

- *plug-and-play modeli*, koji omogućavaju brzo korišćenje gotovih alata;
- *AI as a Service* (AIaaS) što podrazumeva da kompanije koriste već razvijene AI sisteme preko interneta i prilagođavaju ih svojim potrebama;
- *custom AI modeli*, koji se razvijaju od nule za specifične procese i podatke, pružajući maksimalnu preciznost i kontrolu.

NAJČEŠĆA UPOTREBA VEŠTAČKE INTELIGENCIJE U POSLOVANJU

Veštačka inteligencija više nije samo trend već standard u poslovanju. U nastavku su primeri najčešćih praktičnih primena AI danas:

Sajber bezbednost - AI sistemi otkrivaju neuobičajena ponašanja, pokušaje hakerskih napada i potencijalne bezbednosne propuste mnogo brže nego klasične metode, čime značajno smanjuju rizik od incidenata.

Prodaja - AI analizira kupovne navike, prepoznaje obrasce i predviđa potražnju, pomažući prodajnim timovima da kreiraju efikasnije ponude

Korisnička podrška - Čatbotovi i virtuelni asistenti omogućavaju korisnicima da 24/7 dobiju odgovore, ubrzavaju rešavanje problema i rasterećuju ljudski tim.

Marketing - Algoritmi analiziraju podatke o ponašanju korisnika i kreiraju personalizovane kampanje, što povećava efikasnost oglašavanja i smanjuje troškove.

Optimizacija lanca snabdevanja i logistike – AI predviđa zalihe, optimizuje rute, smanjuje troškove transporta i pomaže kompanijama da brže odgovore na promene potražnje.

Izbor nivoa zavisi od veličine kompanije, resursa i ciljeva. Manja preduzeća češće se oslanjaju na *plug-and-play* ili *AIaaS*, dok se za kompleksne potrebe razvijaju custom modeli.

Ovo je tek početak uticaja i primene veštačke inteligencije i može se pretpostaviti da će u budućnosti biti mnogo prisutnija i na taj način još više transformisati sve sektore poslovanja. Neprihvatanje AI, znači reći ne budućnosti i inovacijama. Ona se može posmatrati kao ”duša” informacionih tehnologija, jer one postoje da bi olakšale čoveku rad i smanjile utrošak sati, a veštačka inteligencija daje dodatnu vrednost automatizaciji procesa.

« POVRATAK NA SADRŽAJ

POSLOVNI AI ALATI KAO PARTNERI U RADU

Piše:
Nikola Ostojić,
IN2 Beograd

U poslovnom svetu pratimo kako se alati zasnovani na veštačkoj inteligenciji uklapaju u svakodnevni rad i već sada koristimo dve najpopularnije opcije: **ChatGPT** i **Microsoft Copilot**. Njih ne doživljavamo kao zamenu za eksperte, već kao pomoćnike koji ubrzavaju rad, smanjuju rutinske zadatke i omogućavaju da se fokus preusmeri na ono što donosi pravu vrednost.

Microsoft Copilot je posebno koristan zato što je integrisan u **Visual Studio** i druge Microsoft Office alate koje koristimo. Programerima pomaže da brže pišu kod, predlaže rešenja, detektuje potencijalne greške i nudi optimizacije u realnom vremenu. Na taj način oslobađa vreme za složenije zadatke, arhitekturu sistema, kvalitet koda i razmišljanje o korisničkim potrebama.

ChatGPT je, sa druge strane, fleksibilan alat koji koristimo u širem spektru situacija. Može da pomogne u pisanju dokumentacije, sažimanju informacija, kreiranju primera koda, ali i u svakodnevnoj komunikaciji, od jasnijeg sastavljanja mejlova do brze provere ideja. Njegova sposobnost da ponudi različite uglove posmatranja čini ga posebno dragocenim u ranim fazama projekata kada se traže kreativna rešenja i procene.

Pored gore navedenih, korisni su i alati poput **Gamma.app**, koji omogućava brzo i jednostavno kreiranje prezentacija, kao i **Grammarly**, koji pomaže da tekstovi budu jasni, gramatički ispravni i stilistički precizni, na više jezika, čime se olakšava svakodnevna poslovna komunikacija.

Kombinovanom upotrebom ovih alata dobijamo balans između tehničke preciznosti i šire produktivnosti. Na ove tehnologije treba da gledamo kao na partnere u radu, a ne kao na prolazni trend. Takođe, potrebno je analizirati ostale alate koji se nude na tržištu i njihov potencijal da ih implementiramo kod samih korisnika kroz naše aplikacije da bismo olakšali i njihov rad, ali naravno uz jednu dozu rezervisanosti, s obzirom na to da AI modeli, iako već duže vreme popularni, još moraju da “uče”.

UTICAJ AI NA TRŽIŠTE RADA

Piše:
Miloš Turinski
Infostud

Veštačka inteligencija je na tržište rada donela novu dozu uzbuđenja, ali i neizvesnosti. Gotovo da nema dana kada se u poslovnim razgovorima ili u javnosti ne pojavi pitanje: da li će baš moj posao nestati? Taj strah nije nov, pratio je svaku tehnološku revoluciju. Kada su fabrike počele da zamenjuju ručnu izradu, ljudi su mislili da zanati više nemaju smisla. Kada je internet postao svakodnevica, činilo se da više neće biti potrebe ni za šalterima, ni za pisanim pismima. Ali istorija nas uči da poslovi ne nestaju tek tako, oni se transformišu. Isto posmatramo i danas, samo mnogo brže.

Ono što polako odlazi u senku jesu poslovi koji se zasnivaju na rutini i ponavljanju. Nekada je bilo normalno da ljudi sate provode u prepisivanju podataka ili u izradi izveštaja, a danas algoritmi to završe u sekundi. Prvi kontakt sa klijentima često preuzimaju chatbotovi, dok ljudska uloga ostaje tamo gde je potrebno razumevanje i empatija. I upravo tu leži razlika -

AI ne briše ljude sa tržišta rada, već ih oslobađa repetitivnih zadataka i pomera ih ka odgovornijim i kreativnijim ulogama.

Na Infostudu vrlo jasno vidimo kako se promena preliva u praksu. Oglasi za poslove koji pre pet godina nisu ni postojali sada su svakodnevica. Kompanije traže ljude koji umeju da čitaju i upravljaju velikim količinama podataka, da razvijaju i prilagođavaju digitalne proizvode, da se bave sajber bezbednošću ili da obučavaju softverske modele. Pojavljuju se i specijalisti koji pomažu timovima da na najbolji način koriste AI u svom radu. To nisu moderne pozicije iz Silicijumske doline već konkursi koji danas stoje pred kandidatima u Srbiji.

Za nas, najvažnije pitanje nije da li će AI zameniti čoveka, već da li smo spremni da učimo i prilagođavamo se. Mašina teško može da ponovi ljudske osobine - kreativnost, kritičko razmišljanje, sposobnost da razumemo druge ljude i donesemo odluku na osnovu nijansi. Upravo tu leži naša prednost. Kompanije koje to razumeju neće gledati na AI kao na konkurenciju, već kao na partnera zaposlenih - alat koji oslobađa prostor da ljudi rade ono u čemu su nezamenjivi.

Zato AI ne donosi kraj posla, već kraj rutine.

On završava ono što nam je do juče trošilo sate, a nama ostavlja priliku da radimo pametnije i smislenije. Ako nas istorija nečemu uči, to je da nijedna tehnološka promena nije ukinula rad, već ga je oblikovala. Tako će biti i sada. Najveći kapital i dalje ostaje čovek - samo što su mu alati pametniji nego ikada.

« POVRATAK NA SADRŽAJ

SIGURNOST KOJA MISLI I UČI SA NAMA

PULSEC
Powered by Telekom Srbija

Kako su stvorili prvi AI alat u regionu za borbu protiv digitalnih pretnji i kako taj alat funkcioniše u realnim situacijama, za **BeRiskProtected** govore

Sanja Rakić, kompanija **Pulsec** i
Ivan Kadić, kompanija **Reputeo**.

Na konferenciji Pulse360 predstavljen je AI security asistent – AISA. Ovaj revolucionarni alat postaje sastavni deo Security Operations Centra (SOC), menjajući način na koji se odgovara na bezbednosne pretnje.

Kako je nastala AISA i šta je bila početna ideja?
Sanja Rakić: AISA je nastala iz svakodnevne potrebe našeg SOC tima: da podignemo fokus sa ručnih, ponavljajućih koraka na razumevanje priče iza signala. Želeli smo asistenta koji ne samo da prikuplja podatke, već ih povezuje u smislen kontekst i predlaže naredne korake. Vidimo rast tražnje za SOC uslugama (Security Operations Center) koje podrazumevaju nadzor 24/7 i detekciju bezbednosnih incidenata. To uključuje nadgledanje mreže, servera, aplikacija i korisnika, uz stalnu analizu i brzo reagovanje na potencijalne pretnje. AISA je postala prvi „kolega“ koji sustiže tempo pretnji, ali ostavlja ljudima prostor da donose odluke sa više poverenja. Nije ideja da radimo bilo kakvu zamenu čoveka veštačkom inteligencijom, ideja je da olakšamo rad analitičarima i da poboljšamo uslugu koju pružamo našim klijentima.

Šta AISA konkretno radi u svakodnevnom radu SOC-a i koji su prvi benefiti?
Ivan Kadić: AISA obogaćuje tikete relevantnim podacima (logovi, reputacija indikatora, prethodne slične situacije), koreliše udaljene događaje i izdvaja ono što menja prioritet. Umesto skakanja kroz alate, analitičar dobija koherentan narativ incidenta i jasnu listu preporuka, zajedno sa tragom objašnjenja. Zahvaljujući ovim benefitima, uz rad SOC-a, AISA omogućava da se pretnje uoče ranije, da se brže reaguje, da se brže vidi ako je neko u sistemu korisnika. Manja je zagušenost tima, brže sazrevanje procene rizika i bolja saradnja sa poslovnom stranom, jer govorimo jezikom uticaja na operacije.

Da li možete da podelite neki primer iz poslovne prakse?
S. Rakić: Desila se phishing kampanja koja je ciljala nekoliko naših zaposlenih. Bez AISA-e, analitičarima je trebalo više od sat vremena da povežu sumnjive e-mailove, logove sa e-mail gateway-a i prijave korisnika. Sa AISA-om, sve te informacije bile su korelisane u startnom tiketu, phishing domen je već imao reputacionu oznaku, link je prošao sandbox analizu i odmah je sugerisano da incident nije izolovan.

Detekciju i reakciju smo sa sat vremena skratili na svega desetak minuta.

Reagovali smo mirno i ciljano. Najvredniji rezultat bio je osećaj da tim kontroliše situaciju i da svako zna svoj sledeći potez.

Kako adresirate rizike AI-a: halucinacije, pogrešne korelacije i „crnu kutiju“?
I. Kadić: AISA je projektovana oko principa objašnjivosti i auditabilnosti: svaka preporuka ima jasan trag, referencu i mogućnost ljudske intervencije. Modele treniramo na verifiko-

vanim slučajevima, a povratna informacija analitičara ulazi u kontinuirano učenje, čime smanjujemo rizik od preteranog poverenja u automatizaciju. Time gradimo poverenje i postavljamo standard da je transparentnost dizajn-princip, a ne marketinška fraza.

Šta AI menja u odnosu bezbednosti i biznisa – kako ubrzava odluke?
S. Rakić: AI u bezbednosti nema vrednost ako ne pomaže poslovnim odlukama: prioriteti, procena uticaja, komunikacija sa menadžmentom. AISA prevodi tehničke nalaze u jasan poslovni kontekst. U bankarstvu i osiguranju ne postoji luksuz dugog premišljanja. Kada AISA spoji anomalije u pristupu, reputaciju domena i obrazac transakcije, dobijamo jasan poslovni kontekst i preporuku. Tako donosimo brže i sigurnije odluke, bez buke. U bankama i osiguranju najviše pomaže modularnost: priključimo se na postojeće KYC/AML i core sisteme bez teških migracija. AISA ne 'iznosi' podatke izvan politike kuće; radimo lokalno, sa kompletnim audit tragovima za regulatora i osiguravača. To je način da inovacija ostane usklađena. Znamo šta je ugroženo, u kojem roku, koji su troškovi nečinjenja, pa ključni ljudi brže razumeju posledice i opcije.

U praksi, to znači bržu i sigurniju eskalaciju, ali i manje šuma oko incidenata niskog rizika.

Gde vidite glavne rizike i kako AISA pomaže?
I. Kadić: Kako se pojave digitalnih identiteta, udaljene saradnje i 3D okruženja šire, površina napada postaje kompleksnija – posebno u domenu identiteta i pristupa. AISA pomaže da sve te slojeve posmatramo kao jedinstvenu priču: korisnik–uređaj–sesija–transakcija, uz rano uočavanje odstupanja i neobičnih putanja pristupa. Fokusiramo se na signal kohezije i integritet identiteta, jer u mešovitom svetu rada upravo tu nastaju najskuplje greške.

Kako AI i AISA utiču na povrat ulaganja i osiguranje?
I. Kadić: Kada je proces reagovanja predvidljiv i objašnjiv, lakše je dokazati usklađenost i pregovarati o povoljnijim polisama sajber osiguranja. AISA pomaže evidencijom odluka i audit tragovima, što je važno za due-diligence i regulativu, ali i za upravljanje reputacionim rizikom u finansijskom sektoru. Na strani prodaje, brže čišćenje incidenata održava dostupnost usluga i poverenje klijenata – to je vrednost koju poslovna strana jasno prepoznaje.

Kako obezbeđujete privatnost i zaštitu podataka?
S. Rakić: Ne pravimo kompromise oko zaštite podataka i prava korisnika: minimalni obim obrade, lokalno usklađeno čuvanje i potpuna revizija pristupa. Ljudska kontrola nad kritičnim odlukama je obavezna, a preporuke AI-a moraju biti razumljive onome ko potpisuje rizik. Tako čuvamo suštinu poverenja – korisnika i regulatora - odgovornost pre efikasnosti.

Šta je sledeće na mapi puta – integracije, skaliranje i različite regulative?
I. Kadić: Gradimo modularne konektore i „plug-and-play" pristup da se AISA uklopi tamo gde tim već radi, bez teških migracija. Uvedeni su standardi merenja kvaliteta po okruženju i kompletni audit tragovi, kako bismo lakše ispunili zahteve različitih jurisdikcija i internih politika. Naša ambicija je proaktivan SOC koji raste sa organizacijom i novim poslovnim modelima, a ne rešenje koje je „fiksirano" za jedan alat. U narednoj fazi planiramo da AISA postane platforma koja se može koristiti i van QRadara i ServiceNow-a, odnosno da se integriše sa drugim alatima koje koriste analitičari širom industrije.

« POVRATAK NA SADRŽAJ

METAVERZUM: TEHNOLOŠKA EVOLUCIJA I DRUŠTVENI UTICAJ

Autori:
Dr Marija Marković Blagojević
Univerzitet Singidunum, Beograd

Dr Nikola Radić
Visoka škola za poslovnu ekonomiju i preduzetništvo, Beograd

Dr Milena Cvjetković
Visoka škola akademskih studija „Dositej“, Beograd

Metaverzum predstavlja novu fazu tehnološkog razvoja koja spaja virtuelnu stvarnost, proširenu stvarnost, blockchain i veštačku inteligenciju i tako stvara imerzivna digitalna okruženja. Kroz razvoj virtuelnih svetova i napredak u tehnologiji, Metaverzum postaje sve prisutniji, pružajući bogatija iskustva socijalizacije i ekonomske mogućnosti, ali istovremeno izaziva zabrinutost u vezi sa privatnošću, sigurnošću i zavisnošću od medija. Nacionalne politike i stavovi međunarodnih organizacija takođe igraju ključnu ulogu u oblikovanju budućnosti Metaverzuma.

ISTORIJSKI KONTEKST

Termin „metaverse“ prvi put je upotrebio Nil Stivenson u svom romanu “Snow Crash” iz 1992, koji se od fiktivne ideje razvio u stvarnost. Rani virtuelni svetovi, poput Second Life-a i MMORPG-ova (Massively Multiplayer Online Role-Playing Games), postavili su temelje za složenija virtuelna okruženja. Trenutne platforme poput Robloxa i Fortnite-a smatraju se pretečama Metaverzuma.

Početkom 2000-ih, virtuelni svetovi poput Second Life-a omogućili su korisnicima da kreiraju avatare, grade virtuelne domove i učestvuju u ekonomskim aktivnostima koristeći virtuelnu valutu koja se mogla zameniti za stvarni novac. Međutim, za ove rane platforme postojala su tehnološka ograničenja poput propusne moći i procesorske snage računara. Danas, napredak u hardveru, kroz VR naočare i opremu, poput Oculus Rift-a i HTC Vive-a, zajedno s poboljšanjima u internet infrastrukturi, omogućili su razvoj sofisticiranijih i imerzivnijih virtuelnih okruženja. Uspon blockchain tehnologije dodatno je proširio mogućnosti unutar Metaverzuma, omogućavajući stvaranje decentralizovanih virtuelnih ekonomija gde korisnici mogu sigurno posedovati digitalna sredstva i trgovati njima.

TEHNOLOŠKE OSNOVE

Blockchain koji služi kao ekonomska osnova Metaverzuma, omogućava decentralizovan sistem knjigovodstva koji osigurava bezbedno vlasništvo i trgovanje digitalnim sredstvima bez potrebe za posrednicima.

NFT-ovi (nezamenljivi tokeni), koji predstavljaju vlasništvo nad jedinstvenim digitalnim objektima, prikazuju kako se blockchain primenjuje u Metaverzumu, omogućavajući kreatorima da unovče svoje digitalne kreacije, poput virtuelne imovine i digitalne umetnosti.

Veštačka inteligencija (AI) igra ključnu ulogu u Metaverzumu omogućavajući stvaranje realističnih avatara i složenih interakcija unutar tog okruženja. Osim toga, AI analizira podatke korisnika kako bi personalizovao iskustva.

Proširena i virtuelna stvarnost - VR naočare korisnike prenose u virtuelne svetove, dok AR preklapa digitalni sa-

držaj na fizičkom okruženju, čineći digitalne interakcije intuitivnim i realnim.

Računarstvo na ivici (Edge Computing) smanjuje kašnjenje i poboljšava performanse aplikacija u Metaverzumu. Omogućava brzu obradu podataka blizu mesta gde se generišu, što je ključno za aplikacije u realnom vremenu kao što su AR i VR.

Računarstvo u oblaku (Cloud Computing) obezbeđuje kapacitete za skladištenje i obradu podataka, omogućavajući kompleksne operacije i kolaboraciju u realnom vremenu.

Mreže sledeće generacije (5G i 6G) omogućavaju brze i pouzdane veze koje su neophodne za funkcionisanje Metaverzuma.

Internet stvari (IoT) omogućava povezivanje fizičkog sveta sa digitalnim prostorom. Senzori i uređaji prikupljaju podatke iz stvarnog sveta i šalju ih u Metaverzum radi obrade i interpretacije.

DRUŠTVENI UTICAJI

Samoprikazivanje i socijalizacija: Metaverzum nudi nove načine za izražavanje putem prilagodljivih avatara i virtuelnih postavki. Korisnici mogu kreirati i nastaniti prostore koji odražavaju njihovu ličnost i interese, podstičući osećaj zajedništva i pripadnosti. Platforme kao što su VRChat

« POVRATAK NA SADRŽAJ

i Rec Room, omogućavaju korisnicima da dizajniraju svoje avatare i virtuelna okruženja, što rezultira jedinstvenim socijalnim interakcijama i formiranjem virtuelnih zajednica.

Ekonomske mogućnosti: Očekuje se da će digitalna ekonomija unutar Metaverzuma rasti, vođena trgovinom virtuelnih dobara, nekretnina i usluga. NFT-ovi igraju ključnu ulogu u ovom ekosistemu, omogućavajući kreatorima da monetizuju svoje digitalne kreacije. Virtuelne tržišne platforme, poput Decentraland-a i The Sandbox-a, omogućavaju korisnicima da trguju virtuelnim zemljištem i sredstvima, stvarajući nove ekonomske prilike i poslovne modele.

Privatnost i bezbednost: Kako korisnici budu provodili više vremena u Metaverzumu, zabrinutost zbog privatnosti podataka i bezbednosti će rasti. Velika količina prikupljenih ličnih podataka može biti zloupotrebljena ako nije adekvatno zaštićena. Obezbeđenje snažnih mera privatnosti i transparentnih politika o podacima je od suštinskog značaja.

Pitanja poput „curenja" podataka, krađe identiteta i nadzora treba rešiti kako bi se očuvalo poverenje korisnika.

Zavisnost od medija: Imerzivna priroda Metaverzuma može pogoršati probleme u vezi sa zavisnošću od medija. Studije su pokazale da igranje u virtuelnoj stvarnosti može biti zaraznije od tradicionalnih video igara, što izaziva zabrinutost zbog dugoročnih efekata na mentalno zdravlje i socijalno blagostanje.

BUDUĆI PRAVCI I PREPORUKE

Regulacija i politika: Vlade i regulatorna tela treba aktivno da prate razvoj Metaverzuma i usvoje odgovarajuću regulativu kako bi zaštitile prava korisnika, podstakle konkurenciju i obezbedile transparentnost u poslovanju tehnoloških kompanija. Regulacija bi trebalo da obuhvati oblasti kao što su privatnost podataka, bezbednost, ekonomska jednakost i dostupnost.

Obrazovanje i svest: Edukacija o potencijalnim rizicima i koristima Metaverzuma trebalo bi da bude prioritet kako bi se korisnici osnažili da donose informisane odluke o svom učešću u virtuelnom svetu.

Imerzivno iskustvo

Iskustvo u kojem korisnik oseća da je potpuno uronjen u virtualno ili fizičko okruženje, do te mere da postaje deo tog okruženja i zaboravlja na stvarni svet oko sebe. To se postiže kroz kombinaciju tehnologija kao što su virtualna realnost (VR), proširena realnost (AR), zvučni efekti i interaktivni elementi koji zajedno stvaraju osećaj prisustva i angažovanja

Razvijanje digitalne pismenosti, posebno među mladima, pomoći će u smanjenju ranjivosti na zloupotrebu i negativne uticaje Metaverzuma.

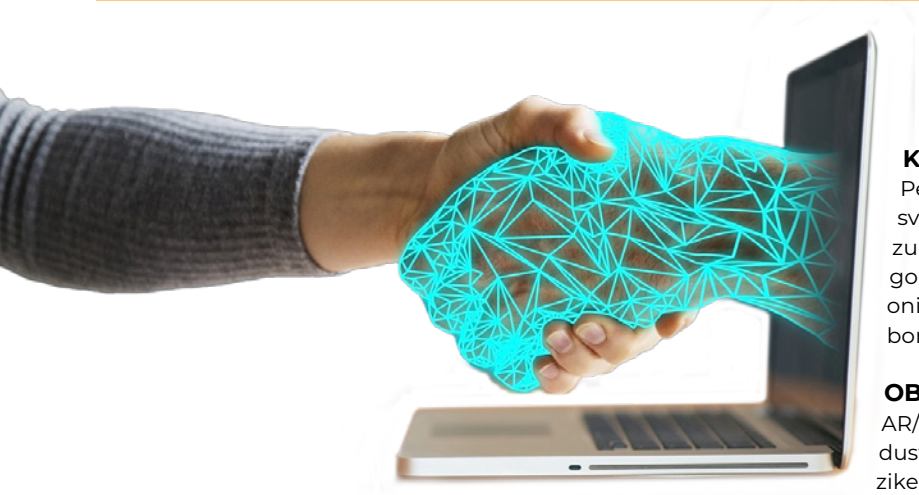
Etika i odgovornost: Tehnološke kompanije koje razvijaju Metaverzum imaju odgovornost da integrišu etičke principe u dizajn i upravljanje platformama. Ovo uključuje transparentno postupanje sa korisničkim podacima, zaštitu privatnosti, suzbijanje štetnih aktivnosti poput zlostavljanja i eksploatacije, kao i promociju inkluzivnosti i raznolikosti.

Interdisciplinarni pristup: Razvoj Metaverzuma zahteva interdisciplinarni pristup koji uključuje stručnjake iz različitih oblasti, npr.: oblasti tehnologije, psihologije, sociologije, prava i drugih relevantnih disciplina. Sveobuhvatno razumevanje i sagledavanje različitih aspekata Metaverzuma pomoći će u identifikaciji i rešavanju kompleksnih izazova koji predstoje.

Korisničko učešće: Korisnici bi trebalo da imaju mogućnost da aktivno doprinose oblikovanju virtuelnih svetova, učestvuju u procesima donošenja odluka i izraze svoje potrebe i želje. Ovo će pomoći u stvaranju inkluzivnog i korisnički orijentisanog Metaverzuma koji odražava raznolike perspektive i interese svojih korisnika.

**Izvod iz rada*
„Metaverzum: tehnološka evolucija i društveni uticaj"
objavljenog u naučno stručnom časopisu
„Trendovi u poslovanju"

KAKO METAVERZUM UNAPREĐUJE BIZNIS



KORISNIČKO ISKUSTVO

Personalizovana, interaktivna iskustva u AR/VR svetu povećavaju lojalnost kupaca. Metaverzum omogućava da se ponuda potpuno prilagodi kupcima i njihovim željama, posebno što oni ostavljaju veliki broj podataka tokom svog boravka.

OBUKA I EDUKACIJA ZAPOSLENIH

AR/VR se koristi za simulacije (npr. medicina, industrija, bezbednost), što smanjuje troškove i rizike. Metaverzum pruža iskustvo koje je jako približno realističnim scenarijima te se predviđa da će značajno izmeniti obuke i edukaciju zaposlenih u pojedinim oblastima. Doktori, na primer, mogu koristiti VR simulacije za vežbanje operacija, dok inženjeri mogu koristiti VR za obuku na mašinama ili uređajima koji su skupi i teško dostupni u stvarnom svetu.

PRODAJA I MARKETING

Kompanije već testiraju virtuelne prodavnice, 3D prikaz proizvoda i „virtual try-on“ (vizuelni prikaz kako neki proizvod izgleda na kupcu, odeća, cipele, šminka) opcije koje menjaju način kupovine. Osim toga što mogu da kreiraju sopstvena prodajna mesta u virtuelnom svetu, brendovi se mogu u njima i reklamirati velikom broju korisnika širom planete. Trenutno je najpopularnije reklamiranje u video igricama. Južnokorejski proizvođač automobila Hyundai je kreirao sopstveni igricu u Robloxu, kao deo metaverse marketinške kampanje, u kojoj su sva vozila upravo brenda Hyundai. Gucci je pre četiri godine kreirao digitalne cipele The Gucci Virtual 25 koje su se mogle nositi u aplikacijama Roblox i VRChat, a cena je bila 12,99 dolara, dakle mnogo manje nego u realnom svetu. Samo Robloksu dnevno pristupi u proseku više od 40 miliona ljudi, među kojima dominiraju Generacija Z i Milenijalci.

RADNO OKRUŽENJE

Virtuelne kancelarije i sastanci u metaverzumu mogu promeniti način na koji timovi globalno sarađuju. Sa trendom hibridnog rada i rada od kuće, metaverzum omogućava povezivanje zaposlenih. Već postoje platforme unutar kojih zaposleni kreiraju svoje avatare. Oni ulaze u virtuelne kancelarije ili sale za sastanke, održavaju prezentacije ili pak samo uživaju sa kolegama u prostoriji za druženje.

NOVI POSLOVNI MODELI

Pojava „virtual real estate“, digitalne robe i NFT-a kao sredstava razmene i statusa omogućavaju da se osmisle i potpuno novi poslovni modeli i kreira dodatni izvor zarade.

« POVRATAK NA SADRŽAJ

RIZICI I POTENCIJALNA OSIGURANJA U METAVERZUMU

Piše:
Dr Branko Pavlović
član IO Globos osiguranja

Metaverzum je futuristički digitalni svet koji postoji paralelno sa našim svetom – ukratko, to je meta-univerzum. Najsličniji je kompjuterskim igricama. Potencijal metaverzuma je toliko veliki da je inspirisao jednu od najvećih svetskih tehnoloških kompanija, Facebook, da krajem 2021. godine promeni ime u Meta Platforms.

Metaverzum nudi velike mogućnosti za osiguravače i reosiguravače u upravljanju rizikom imovine stvarnog i virtuelnog života.

Sve veća popularnost metaverzuma stvara niz novih rizika koji imaju finansijske implikacije u stvarnom svetu. Veoma mali broj ovih rizika može trenutno biti pokriven osiguranjem, što osiguravačima daje mogućnost za kreiranje novih proizvoda koji štite imovinu i lica i u stvarnom i u virtuelnom svetu, što podrazumeva zaštitu digitalne imovine i NFT-a, digitalnih identiteta, osiguravanje kontinuiteta poslovanja i zaštite intelektualne svojine za mnoge kompanije koje upravljaju delovima metaverzuma. Pored toga, osiguravači mogu da igraju ulogu i u rešavanju potencijalnih problema koji proizilaze iz upotrebe same tehnologije štiteći stvarni svet od nekih potencijalnih rizika koje metaverzum može predstavljati (od maltretiranja na internetu do problema zavisnosti). Investitorima, kupcima i kreatorima u metaverzumu potrebna je efikasna za-

štita po pristupačnoj ceni od potencijalnog finansijskog gubitka, odgovornosti i gubitka mogućnosti za korišćenje sopstvene imovine.

ŠTA ĆE MOĆI DA SE OSIGURA

Novi rizici specifični za metaverzum, koji će u budućnosti moći da budu osigurani, su sledeći: gubici usled tehnoloških problema kao što su loše programirani događaji u metaverzumu, ograničeni kapaciteti računarske mreže, nemogućnost pristupa internetu i prekidi usluga provajdera, koji mogu uzrokovati finansijske gubitke korisnicima, platformama, brendovima, kompanijama i promoterima događaja; kriminalno i zlonamerno ponašanje u virtuelnom svetu slično sajber rizicima u realnom svetu; finansijske prevare koje se odnose na lažne virtuelne nekretnine, ilegalno prikupljanje sredstava i različite nedozvoljene aktivnosti sa kripto valutama; hakovanje radi krađe ličnih podataka iz realnog sveta, podataka o avatarima i druge virtuelne imovine ili uništenja VR opreme; krađe identiteta (avatara), virtuelnih nekretnina i druge digitalne imovine; kršenja autorskih prava u VR, koja izazivaju finansijski gubitak i gubitak poverenja klijenata, vlasnika i kreatora; mentalni problemi lica koji mogu nastupiti usled uznemiravanja na mreži, trolovanja i toksičnih ponašanja koja nanose emocionalne bolove.

Za osiguravajuće kompanije trenutno postoje tri moguće ulazne tačke za osiguranje rizika u metaverzumu: digitalna sredstva u metaverzumu, događaji i zabava, i intelektualna svojina i brend.

NFT, avatari i virtuelne nekretnine su virtuelna sredstva koja imaju novčanu vrednost u stvarnom svetu. Njihovim vlasnicima je potrebna zaštita od gubitka. Virtuelne nekretnine suočavaju se sa rizicima od krađe i hakovanja, kao i sa rizicima od sajber vandalizma. Vlasnici nekretnina u metaverzumu mogu doživeti finansijsku i reputacionu štetu, banke kreditori vlasnika tih nekretnina mogu izgubiti prihod, dok se operateri virtuelnih platformi na kojima je uspostavljen metaverzum mogu suočiti sa tužbama za kompenzaciju od obe grupe.

Nekoliko poznatih ličnosti i restorana već su bili domaćini koncerata, modnih revija i drugih događaja u metaverzumu. Broj događaja i učesnika se povećava, što dovodi do većeg rizika u vezi sa otkazivanjem događaja, kašnjenjem ili kvalitetom, kao i bezbednošću učesnika. Postoji očigledna prilika za osiguravače da uvedu u metaverzum zaštitu: učesnika na događajima u slučaju otkazivanja, kašnjenja, finansijskog gubitka i drugih problema koji nisu bili njihova krivica; organizatora i izvođača od gubitka reputacije, finansijskog gubitka ili tužbi učesnika u vezi sa bilo kojim problemom sa događajem; pružalaca usluga obezbeđenja platformi za virtuelne događaje od tužbi organizatora, izvođača i učesnika zbog grešaka ili problema u prenosu događaja preko interneta.

U metaverzumu postoji i rizik od kršenja i zloupotrebe sadržaja, žigova i autorskih prava poznatih ličnosti i brendova. To znači da postoji realna mogućnost finansijskog gubitka i štete po reputaciju za vlasnike metaverzum platformi, ljude i institucije koji ih koriste i one koji imaju prava intelektualne svojine. Provajderi platformi za metaverzum i tržišta rizikuju da budu tuženi zbog ovih kršenja prava nad intelektualnom svojinom, tako da su zainteresovani za ponudu osiguranja od odgovornosti za to.

« POVRATAK NA SADRŽAJ

AI I RIZICI PO PRIVATNOST

Da se veštačka inteligencija razvija brže nego što regulativa može da je prati nije nikakva tajna. Ali dok s jedne strane uživamo u blagodetima koje nam tehnologije donose, sve češće se postavlja pitanje na koje sve načine možemo da budemo ugroženi.

Stoga je prošle godine organizacija OECD koja okuplja 38 razvijenih zemalja (koje zajedno pokrivaju većinu svetske trgovine i digitalnih tržišta), i koja se još od 70-tih godina prošlog veka bavi politikom zaštite podataka i transnacionalnim protokom informacija, usvojila izveštaj **„AI, Data Governance & Privacy: Synergies and Areas of International Co-operation“** (OECD, jun 2024). S obzirom na to da AI prelazi granice (cloud, podaci, algoritmi, kompanije rade globalno), i da se nacionalni zakoni razlikuju (npr. EU ima GDPR, SAD nema jedinstven federalni zakon), ovaj izveštaj je ponudio platformu za harmonizaciju standarda odnosno globalne smernice koje mogu da postanu osnova za zakone i regulative u državama članicama (a često i šire).

Cilj izveštaja je da istraži preseke između AI i privatnosti: da identifikuje rizike i mogućnosti, da poveže postojeće principe zaštite podataka sa principima AI, i da predloži oblasti međunarodne saradnje u politici i regulaciji.

RIZICI KOJE AI DONOSI U POGLEDU PRIVATNOSTI

Izveštaj identifikuje sledeće ključne rizike:

Neovlašćeno prikupljanje i upotreba podataka za treniranje modela: AI sistemi često koriste ogromne skupove podataka, uključujući lične podatke sa javno dostupnih izvora, što može prekršiti principe zakonitog, poštenog i transparentnog prikupljanja podataka.

Izvođenje zaključaka, profilisanje i predikcija: AI modeli mogu iz podataka da izvuku osetljive karakteristike pojedinaca (npr. pol, rasu, starost...) čak i kad ti podaci nisu direktno prisutni, što otvara rizike diskriminacije i nekorektnog profilisanja.

Deanonimizacija / reidentifikacija: čak i ako su pojedinačni podaci anonimni ili pretvoreni u pseudonime, tehnike analize velikih podataka i ponašanja modela mogu dovesti do vraćanja identiteta pojedinaca (reidentifikacija).

Nedostatak transparentnosti („black box“ modeli): načine na koji modeli donose odluke teško je objasniti, a to otežava korisnicima da razumeju ili ospore automatske zaključke.

Prava na ispravku, brisanje i povlačenje pristanka: kod modela koji su trenirani na istorijskim podacima, čak i ako korisnik želi da obriše ili ispravi svoje podatke, može biti tehnički komplikovano „odučiti“ model od tih podataka.

Halucinacije i pogrešne informacije / obmanjujući rezultati: AI može generisati neistinite ili netačne informacije koje mogu kršiti privatnost ili širiti dezinformacije.

Akumulacija moći i kontrole nad podacima: kompanije koje kontrolišu veliki broj podataka i AI infrastrukturu mogu da steknu dominantnu poziciju, što može ograničiti konkurenciju i slobodu korisnika u odlučivanju o svojim podacima.

SMERNICE I PRINCIPI ZA ZAŠTITU PODATAKA

Pozivajući se na smernice za zaštitu privatnosti (Privacy Guidilines) usvojene 1980. a revidirane 2013. godine, i na principe za AI usvojene 2019. a ažurirane 2024. godine (Recommendation on AI), ovaj izveštaj naglašava da

AI treba da bude korisna za ljude i planetu (inclusive growth, sustainable development, well-being), poštena i transparentna, sigurna i pouzdana, da obezbeđuje odgovornost onih koji je razvijaju i koriste i da promoviše upravljanje rizicima.

Države bi trebalo da poštuju prava, ljudska prava i demokratske vrednosti uključujući i pravo na privatnost, zatim da sistemski upravljaju rizicima kako bi obezbedile sigurnost i bezbednost građana, ali i da investiraju u istraživanja i razvoj koji uključuju skupove podataka, ali uz poštovanje privatnosti.

Smernice i principi praktično služe kao "globalni minimum" i zajednički jezik oko privatnosti i AI, kako bi države, regulatori, kompanije i međunarodne organizacije mogli lakše da se usklade i sarađuju. Ne obavezuju nikoga direktno, ali im je svrha da oblikuju politike, zakone i regulative i da pomognu da se izbegne pravni haos i fragmentacija između različitih zemalja.

PREDLOŽENE FORME MEĐUNARODNE SARADNJE

Izveštaj predlaže državama da usaglase pravne i tehničke okvire, da dalje zajednički razvijaju smernice i tehničke alate, da razmenjuju iskustva i kapacitete nadzornih tela, da uvode mehanizme za periodično ažuriranje smernica u skladu sa tehnološkim razvojem i novim rizicima, i naravno – da vrlo glasno informišu javnost kako o rizicima tako i o napretku u sprečavanju da se rizici ostvare.

Izvor: **OECD**

« POVRATAK NA SADRŽAJ

ZAKON O ZAŠTITI PODATAKA O LIČNOSTI – IZAZOVI ZA KOMPANIJE I KAKO IH PREVAZIĆI

Piše:
Petar Mijatović
MIJATOVIĆ LAW Office

Posle više od šest godina primene Zakona o zaštiti podataka o ličnosti (ZZPL), u praksi su se iskristalisali najčešći izazovi, odnosno poteškoće sa kojima se kompanije suočavaju prilikom njegove primene, kao i promene koje bi trebalo inkorporisati kako bi se ti izazovi prevazišli.

I. NEKONZISTENTNOST ODREDBI ZZPL-A I NEUSAGLAŠENOST SA DRUGIM ZAKONIMA

Iako je ZZPL u svom normativnom delu pretežno usklađen sa Opštom uredbom EU o zaštiti podataka o ličnosti (GDPR), zakon ne sadrži uvodne odredbe (recitale) koje su se u EU praksi pokazale kao ključne za razumevanje i sprovođenje GDPR-a. Odsustvo ovih uvodnih odredbi, uz nedostatak adekvatne sudske prakse, otežava tumačenje pojedinih odredbi ZZPL-a. Zbog toga su kompanije često prinuđene da se oslanjaju na recitale GDPR-a i mišljenja Evropskog odbora za zaštitu podataka, iako oni formalno nisu izvori prava u Republici Srbiji.

Takođe, veliki broj posebnih zakona koji regulišu obradu podataka o ličnosti u Srbiji i dalje nije usklađen sa ZZPL-om, iako je član 10. ZZPL-a predvideo da se to mora učiniti najkasnije do kraja 2020. godine.

II. LEGITIMNI INTERES KAO OSNOV ZA DIREKTNI MARKETING

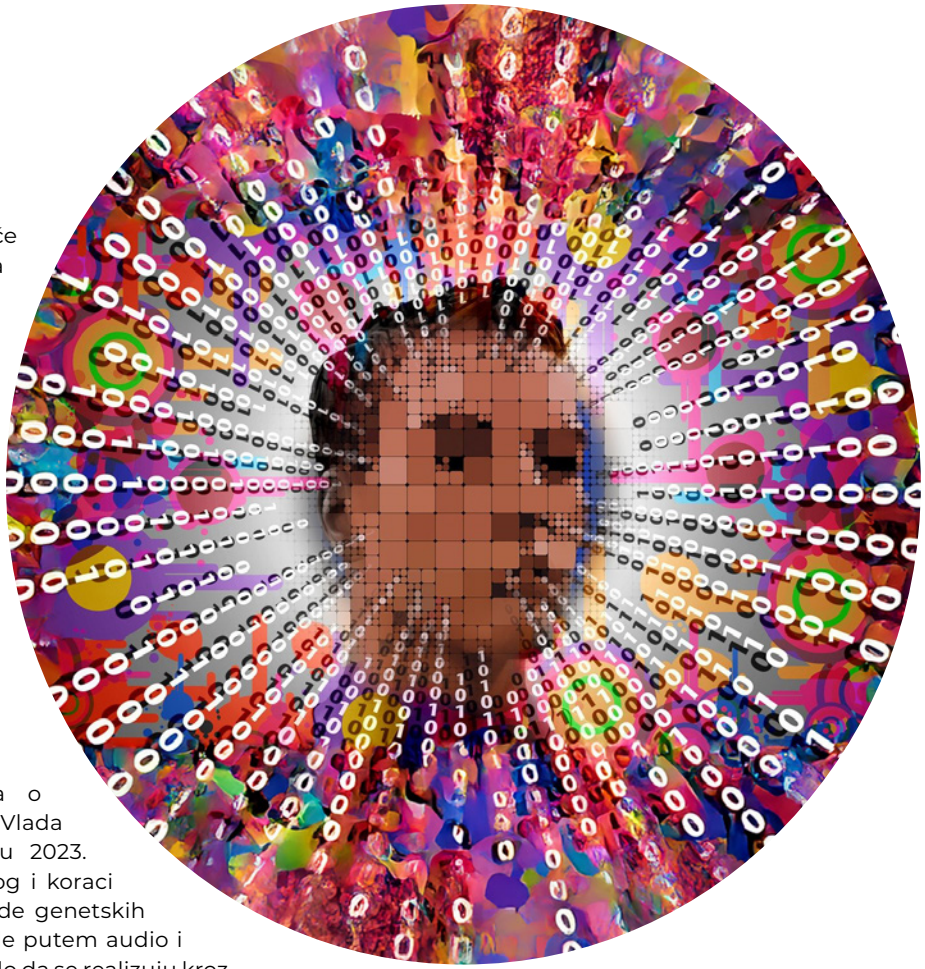
Za razliku od GDPR-a, koji u uvodnim odredbama eksplicitno prepoznaje legitimni interes kao moguć osnov za direktni marketing, ZZPL ovu mogućnost ne razrađuje u dovoljnoj meri. Iako zakon načelno predviđa pravo lica da prigovore obradi svojih podataka u svrhu direktnog oglašavanja — što implicira da obrada može biti zasnovana na legitimnom interesu — posebni zakoni, poput Zakona o oglašavanju, i dalje zahtevaju izričit prethodni pristanak za ovu vrstu obrade.

Usaglašavanje posebnih zakona i prepoznavanje legitimnog interesa ne bi značilo bezuslovnu mogućnost za „spamovanje“ lica, već bi omogućilo da se, uz sprovedenu procenu legitimnog interesa i ispunjene druge uslove, marketing kampanje sprovode prema licima sa kojima je rukovalac već imao određeni poslovni odnos.

III. UVOĐENJE STANDARDNIH UGOVORNIH KLAUZULA ZA SVE TIPOVE PRENOSA PODATAKA

ZZPL trenutno prepoznaje standardne ugovorne klauzule koje izrađuje Poverenik, ali isključivo za odnose između rukovaoca i obrađivača. U praksi to nije dovoljno —

naročito u situacijama kada domaće kompanije imaju status obrađivača u odnosu na inostrane rukovaoce (npr. iz EU), i žele da podatke prenesu svojim podizvođačima (podobrađivačima) u treće zemlje bez adekvatnog nivoa zaštite. Stoga bi, po ugledu na GDPR, ZZPL trebalo izmeniti tako da omogući Povereniku da izradi modele standardnih ugovornih klauzula za sve vrste međunarodnih prenosa: rukovalac–rukovalac, rukovalac–obrađivač, obrađivač–obrađivač i obrađivač–rukovalac.



IV. KORACI PREDVIĐENI STRATEGIJOM ZAŠTITE PODATAKA O LIČNOSTI

Prema Strategiji zaštite podataka o ličnosti za period 2023–2030, koju je Vlada Republike Srbije usvojila u avgustu 2023. godine, predviđeni su između ostalog i koraci ka regulisanju automatizovane obrade genetskih i biometrijskih podataka, kao i obrade putem audio i video nadzora. Ove aktivnosti bi trebalo da se realizuju kroz izmene i dopune ZZPL-a i donošenjem posebnih propisa. Iako su predlozi iz Strategije korak napred, oni bi bili još adekvatniji kada bi uključivali i prethodno pomenute aspekte koji su izuzetno važni za svakodnevno poslovanje kompanija.

V. PLANIRANE IZMENE GDPR-A

Evropska komisija je nedavno predložila izmenu člana 30. (stav 5) GDPR-a, kojom bi se proširilo izuzeće od obaveze vođenja evidencije o radnjama obrade. Trenutno se ovo izuzeće primenjuje na organizacije sa manje od 250 zaposlenih, osim u slučajevima kada postoji veći rizik po prava i slobode pojedinaca.

Prema predlogu, izuzeće bi se odnosilo na organizacije sa manje od 750 zaposlenih, osim ako je obrada takve prirode da je verovatno da nosi visok rizik, u smislu člana 35. GDPR-a.

S obzirom na to da i ZZPL trenutno predviđa isti prag od 250 zaposlenih, bilo bi korisno da se prag poveća i u domaćem zakonodavstvu, čime bi se umanjio administrativni teret, naročito za male i srednje kompanije.

« POVRATAK NA SADRŽAJ

KO JE BRŽI: REGULATIVA ILI AI?

Piše:
Dragan Milić
MILIĆ LEGAL <office&hub>

Utrci sa novom tehnologijom, zakonodavci pokušavaju da održe korak i da postave pravila, pa je Evropska unija prva napravila ozbiljan pomak usvajanjem AI Act-a, Uredbe koja pokušava da uvede AI u koliko-toliko precizno skrojen pravni okvir. Uredba (EU) 2024/1689 Evropskog parlamenta i Saveta od 13. juna 2024. o utvrđivanju usklađenih pravila o veštačkoj inteligenciji (EU AI Act) zvanično je stupila na snagu 1. avgusta iste godine. Cilj je da se postavi globalni standard za AI zasnovan na pouzdanosti, bezbednosti i ljudskim pravima. Ipak, puna primena pravila odvijaće se postepeno, u roku od dve godine počevši od trenutka stupanja na snagu, kako bi se industrija prilagodila novim obavezama.

NIVOI RIZIKA KOJI NOSI AI

Najvažnija odredba koju ovaj Akt donosi predstavlja model klasifikacije zasnovan na nivou rizika, koji će imati uticaj na uslove pod kojima će modeli odnosno sistemi veštačke inteligencije moći da se razvijaju i koriste.

Neprihvatljiv rizik. Na primer, AI sistemi koji manipulišu ponašanjem ili omogućavaju masovni nadzor u realnom vremenu, strogo su zabranjeni.

Visok rizik. Ovi sistemi se koriste u kritičnim oblastima kao što su zdravstvo, pravosuđe, obrazovanje, zapošljavanje i slično.

Ograničen rizik. U ovu grupu spadaju četbotovi, generatori sadržaja i slični alati.

Minimalan ili nikakav rizik. U ovu grupu spadaju AI alati za zabavu, filteri i jednostavni softveri.

AI opšte namene kao posebna kategorija. Modeli poput ChatGPT-a, koji nisu razvijeni za jednu svrhu već imaju širok spektar primene, klasifikovani su kao GPAI — “General Purpose AI”. Za njih važe posebna pravila sa fokusom na transparentnost i sigurnost. Dakle, posebne obaveze važe za sisteme koji imaju veliku računarsku moć i mogu da dovedu do ozbiljnih posledica, odnosno koji nose sistemske rizike.

Eksteritorijalna primena EU AI Act-a

Jedan od ključnih aspekata Akta je njegova eksteritorijalna primena. To znači da se pravila ne odnose samo na subjekte iz EU, već i na one van EU ukoliko njihove AI tehnologije “dolaze” do korisnika unutar Unije ili se rezultat njihovih AI sistema koristi u EU. Za kompanije iz Srbije (i drugih zemalja van EU) to znači da, ukoliko plasiraju svoje AI proizvode ili usluge na tržište EU, moraju biti usklađeni sa pravilima Unije.

PRIMENA I PRAZNINE KOJE TREBA POPUNITI

AI se razvija brže nego što zakon može da odgovori, što je za očekivati. Novi modeli su sve sposobniji i sa sobom nose nepredvidive rizike, od pristrasnosti i dezinformacija do ozbiljnih bezbednosnih rizika. Evropska unija pokušava da svede te rizike na prihvatljivu meru, kroz kodekse dobre

prakse, stručne grupe i tehničke standarde koji se razvijaju paralelno, međutim pitanje je koliko će sve to biti dovoljno i efikasno u ustrojavanju nečega što se vrlo lako može oteti kontroli.

I pored dobre regulatorne osnove koju je doneo AI Act, postoji mnoštvo ozbiljnih izazova na terenu razvoja i korišćenja veštačke inteligencije. Za početak je važno obezbediti sprovođenje postavljenih pravila, jer Uredba bez aparata koji će je sprovoditi i efikasnog nadzora ostaje mrtvo slovo na papiru. Veliki problem čijem rešavanju se trenutno ne vidi konačnica su propisi zemalja koje imaju različite pristupe ovoj problematici, poput SAD i Kine. Tako svetsko tržište ostaje fragmentisano u odnosu na AI, dok se primena i korišćenje sistema AI ne može tako lako ograničiti unutar određenih teritorija i političkih sistema.

I treći, ali ne manje važan izazov je pitanje intelektualne svojine, odnosno prava trećih lica čiji se podaci (u mnogim slučajevima autorska dela) koriste za treniranje modela AI. Tu se naslanja i pitanje zaštite podataka o ličnosti, koji takođe neizbežno ulaze u zonu treniranja i nepovratno se utapaju u dubine algoritama i neuronskih mreža.

Uredba je veliki korak ka regulaciji AI, ali definitivno ne i poslednji. Bez stalnog nadzora, tehničkog unapređenja i međunarodne saradnje, Akt neće moći da ispuni svoju svrhu u potpunosti. A za zemlje poput Srbije, pitanje nije da li, već kada će AI regulativa EU postati i njihova realnost, ne samo kroz eksteritorijalno dejstvo, već i kroz implementaciju u domaće pravo. Kao što se desilo sa GDPR-om, očekuje se da će evropski standardi postati globalna praksa.

« POVRATAK NA SADRŽAJ

VEŠTAČKA INTELIGENCIJA POKREĆE NOVU ERU SAJBER PRETNJI

Piše:
Dragan Davidović
generalni direktor kompanije
Kaspersky za istočnu Evropu

Razvoj i dostupnost alatki veštačke inteligencije značajno su uticali na sajber napade. Generativna AI dodatno je učinila opasnim *spear-phishing* napade - i individualni sajberkriminalci koji ciljaju privatne i finansijske podatke korisnika, i oni najnapredniji koji funkcionišu u okviru organizacija naprednih upornih pretnji (APT), koriste alate za generisanje teksta i chat botove da kreiraju ubedljive i personalizovane *phishing* poruke, pa čak i dokumente ili audio. Ove poruke izgledaju kao da dolaze od poznanika, kolega ili poslovnih partnera i izuzetno su uverljive.

Dark web je preplavljen oglasima koji nude „*deepfake-kao-uslugu*“, a primetna je i jasna potražnja za ovim alatima od strane sajberkriminalaca svih nivoa. Eksplozivni razvoj ovog “crnog tržišta” uzrokovao je i značajan pad cene ovakvih servisa, pa one sada počinju od 50 dolara za lažne video i 30 dolara za falsifikovane glasovne poruke, čineći ih još dostupnijim kriminalcima.

Iako nisu novitet, sve su češći i *ransomware napadi kao usluga (RaaS),* kao i ciljane ransomware operacije. Umesto masovnih napada nasumičnih korisnika, napadi su postali ciljane akcije protiv velikih organizacija – bolnica, država, finansijskog sektora i kritične infrastrukture. U napadima se koristi kombinacija enkripcije i krađe podataka, takozvani *double ili triple extortion*.

Napadi na lance snabdevanja, posebno otvorenog koda, takođe su u porastu, kao i eksploatacije ranjivosti u softveru koji se koristi široko, čak i kada se ne misli da su u prvom planu napada.

Precizni podaci o ukupnim štetama – ekonomskim gubicima, prekidima poslovanja, reputacionoj šteti – generalno su fragmentirani: zavise od sektora, regiona, veličine organizacije, brzine reakcije i drugih faktora. S obzirom na to da smo na pragu četvrtog kvartala, još je rano za podvlačenje crte za ovu godinu. Ipak, za očekivati je da troškovi koje uspešan sajbernapad izazove rastu. Dostupnost sve naprednijeg targetiranja i sve sofisticiranije metode čine da sajberkriminalci nastavljaju da sve više prebacuju fokus na visoko-vredne mete.

Ako znamo da je prošle godine zabeležen porast prosečne zatražene otkupnine za ransomware napad na velike kompanije za 400.000 dolara, jasno je da ne govorimo o simboličnom uvećanju tih iznosa.

Obuke zaposlenih, redovne vežbe, simulacije i ažuriranja ostaju ključna pretpostavka sajberbezbednosti, posebno jer taktike napada stalno evoluiraju. One moraju biti frekventne, ažurirane i uključivati trening u nekoliko ključnih oblasti, kao na primer prepoznavanje fišing

poruka, lažnih linkova, poruka koje koriste socijalni inženjering i generativni AI. Pored toga, od velike je važnosti i obuka za bezbedno korišćenje uređaja, uključujući pametne uređaje, IoT i uređaje koji nisu tradicionalni "računari", jer oni često postaju ciljevi i ulazne tačke. Važno je i da postoji procedura za reakciju na incident i da su sa njom dobro upoznati i zaposleni i timovi za bezbednost. Treninzi koje nudi Kaspersky u okviru svoje **KASAP** platfome (Kaspersky Automated Security Awareness Platform) dostupne na srpskom jeziku adekvatno pripremaju zaposlene o bezbednom ponašanju, ali i kako da prepoznaju prve znakove kompromitovanja, da znaju kome da prijave incident, kako da čuvaju dokaze i kako da izvrše izolaciju sistema.

Za građane je presudna dobra informisanost, oprez i jedna zdrava doza sumnjičavosti prema svemu onome na šta zdrav razum upozorava da izgleda previše dobro da bi bilo istinito. To podrazumeva skeptičnost prema nepoznatim linkovima, porukama i e-mailovima – posebno ako zahtevaju akciju, otvaranje priloga ili unošenje ličnih podataka, čak i ako izgledaju da dolaze od nekog poznatog. Treba razviti i zdrave sajberbezbednosne navike i koristiti višefaktorsku autentifikaciju (MFA) gde god je moguće. Od presudnog značaja su i redovna ažuriranja softvera - operativnih sistema, aplikacija i firmvera uređaja, uključujući rutere i pametne uređaje, jer zapostavljanje ažuriranja često omogućava napadačima da iskoriste poznate ranjivosti. Uz korišćenje pouzdanih bezbednosnih rešenja, treba paziti i na dozvole aplikacija i dodataka za pregledače, jer često "beskorisni" dodaci nose rizik ako imaju pristup podacima ili mogućnost da ih menjaju. Na kraju, važan je i redovan bekap podataka.

« POVRATAK NA SADRŽAJ

DA LI JE VAŠE POSLOVANJE SPREMNO ZA INTELIGENTNE PRETNJE?

Pišu:
Dragan Pleskonjić
Founder&CEO
Glog.AI

Vladimir Jelić
CTO
Glog.AI

Savremeni sajber napadi nisu više samo masovni i generički pokušaji prevare. Danas su oni hirurški precizni, personalizovani i vođeni veštačkom inteligencijom.

Zamislite ovakav scenario: primate imejl od dugogodišnjeg poslovnog partnera, u kojem vas moli za hitnu promenu broja računa za uplatu. Ton, stil pisanja i kontekst poruke su besprekorni. Ne znate da je taj imejl kreirala veštačka inteligencija koja je mesecima analizirala vašu javnu komunikaciju. Vaš finansijski direktor čak dobija poruku izgovorenu tonom glasa i stilom direktora ili vlasnika firme. Ovo je samo jedan primer AI-pokretanih napada. Oni uče, prilagođavaju se i zaobilaze tradicionalne mere zaštite u realnom vremenu. Klasična odbrana, koja se oslanja na prepoznavanje već poznatih pretnji, jednostavno više nije dovoljna.

INTELIGENTNE PRETNJE ZAHTEVAJU INTELIGENTAN ODGOVOR

Na napade vođene veštačkom inteligencijom jedini pravi odgovor je odbrana koja je takođe zasnovana na veštačkoj inteligenciji. To zahteva promenu pristupa: sa reaktivnog na proaktivni i prediktivni.

Shvatajući da se pretnje menjaju iz minuta u minut, razvili smo ekosistem pod nazivom Glogosphere, koji proaktivno predviđa i sprečava napade umesto da čeka da se dese. Bezbednost, po svojoj prirodi, mora biti višeslojna; stoga obezbeđujemo zaštitu na više nivoa.

Moderna odbrana objedinjuje ljude, procese i tehnologiju kroz nekoliko ključnih stubova:

1. Proaktivno delovanje i predviđanje bezbednosnih rizika (Security Predictions): Analizom obaveštajnih podataka o pretnjama, naša rešenja identifikuju potencijalne napade i nove obrasce pre nego što se i dogode, omogućavajući vam da iskoristite moć predviđanja. Ako preduzmete preventivne mere da neutrališete pretnje pre nego što se materijalizuju i naprave štetu, osiguravate da vaša odbrana uvek bude korak ispred.
2. Glog.AI rešenje za bezbednost softvera: Aplikacije i softver koji koristite često su glavna meta i vektor napada. Zato smo razvili platformu zasnovanu na veštačkoj inteligenciji , koja automatski identifikuje i ispravlja ranjivosti softvera tokom procesa razvoja, i pomaže softverskim razvojnim timovima da u ranoj fazi učine softver otpornim na hakerske napade. Tako oni mogu brže da razvijaju inovativne proizvode, bez ugrožavanja bezbednosti.
3. INPRESEC mrežna bezbednost štiti "digitalne puteve" vaše kompanije, tako što osigurava da komunikacija

unutar vaše mreže i sa spoljnim svetom bude bezbedna, sprečavajući, na primer neovlašćeni pristup, uvid, preuzimanje, izmene, brisanje podataka i druge napade. Ovo rešenje inteligentno detektuje anomalije skoro u realnom vremenu, pre nego što nastupi šteta. INPRESEC koristi veštačku inteligenciju da analizira mrežni saobraćaj i tako proaktivno brani vašu mrežu i krajnje tačke, držeći vas uvek korak ispred napadača.

4. Stalni nadzor kroz vSOC: Umesto da teret bezbednosti padne na vaš interni tim, vSOC (Virtuelni bezbednosno-operativni centar) preuzima tu ulogu. To je vaš posvećeni tim vrhunskih stručnjaka koji 24/7 nadgleda vaše sisteme, spreman da reaguje na svaku pretnju u trenutku njenog nastanka.
5. Kroz Penetration testiranje simuliramo realne hakerske napade na vaše sisteme, i tako pronalazimo i zatvaramo „pukotine“ u vašoj odbrani pre nego što ih pravi napadači iskoriste. Ovakvo testiranje prodora, poboljšano veštačkom inteligencijom, nudi efikasniju, sveobuhvatniju i detaljniju identifikaciju ranjivosti, a zatim daje i precizne i delotvorne savete za njihovo otklanjanje.
6. Osnaživanje tima - AI treninzi i obuke u oblasti sajber bezbednosti. Zaposleni treba da razumeju kako funkcionišu moderne pretnje i kako da bezbedno koriste nove tehnologije: tako, oni postaju aktivni čuvari bezbednosti.

U savremenom poslovanju, sajber bezbednost je postala ključna investicija koja obezbeđuje kontinuitet poslovanja, jača poverenje klijenata i podstiče siguran rast.

Neophodno je biti korak ispred napadača, gradeći odbranu koja je inteligentna, brza i sposobna da se prilagodi u skladu sa evoluirajućim pretnjama.

« POVRATAK NA SADRŽAJ

KAKO TELEKOMUNIKACIJE ŠTITE GRAĐANE I KOMPANIJE

Piše:
A1 Srbija

Mikro, mala i srednja preduzeća čine kičmu privrede Srbije: 360.000 registrovanih subjekata, 63% zaposlenih, 99% ukupne privrede. Uprkos toj snazi, većina nema dovoljno resursa da prati tehnološke trendove, zaposli IT stručnjake ili investira u kompleksne sisteme zaštite. Rezultat je da upravo MSP sektor postaje glavna meta sajber napada. Globalno, svako četvrto malo preduzeće već je doživelo incident.

Srbija je među najugroženijim zemljama na svetu: jedan sajber napad dešava se na svakih 39 sekundi, a posebno su pogođeni sistemi upravljanja i kritična infrastruktura.

Iako je svest o rizicima veća nego ranije, tri četvrtine građana i dalje ne zna kako da se adekvatno zaštiti od fišinga i malicioznih sadržaja.

Upravo zato A1 Srbija ulaže u kombinaciju tehnoloških rešenja i edukacije. Platformu #BoljiOnline do sada je posetilo više od 200.000 korisnika, što je najbolji pokazatelj koliko je tržištu potrebna podrška u razumevanju digitalnih pretnji.

Na nivou mreže, rešenja su već donela merljive rezultate. Samo u prvih osam meseci ove godine, servis A1 Net Protect zaustavio je više od **316 miliona pokušaja napada** na mobilne uređaje korisnika. Četvrtina celokupne korisničke baze već koristi ovaj servis, što potvrđuje da tržište prepoznaje vrednost digitalne zaštite kao standarda.

Za biznise, A1 je razvio Cyber Security portfolio koji funkcioniše modularno od zaštite krajnjih uređaja, e-pošte i cloud podataka, do firewall i DDoS sistema. Svaka usluga uključuje Security Operations Center (SOC) kojim se 24/7 nadgledaju ljudi, procedure i tehnologije, i koji po potrebi reaguje na incidente. Time se korisnicima omogućava da fokus ostane na poslovanju, dok stručna podrška u pozadini obezbeđuje sigurnost.

Digitalizacija je drugi ključni izazov za MSP. Mnogi je i dalje vide kao skupu i komplikovanu. A1 nudi drugačiji pristup: postepeni prelazak kroz cloud servise, digitalne alate za saradnju, call centre i IoT rešenja. Svaki korak se gradi modularno, prema realnim potrebama i mogućnostima, čime digitalizacija postaje proces bez rizika i neočekivanih troškova.

Rezultat ovakvog pristupa je da korisnici na jednom mestu dobijaju sve, od pouzdane konekcije, preko ICT i sajber rešenja i ekspertske podrške, do servisne infrastrukture. To A1 pozicionira ne samo kao operatora, već kao partnera koji obezbeđuje sigurnost, kontinuitet i uslove za rast.

Rast složenosti sajber pretnji pokazuje da zaštita više ne može biti odgovornost pojedinca ili malog tima, već zajednički proces u kojem telekomunikacione kompanije imaju značajnu ulogu.

OD ČEGA ŠTITI POLISA SAJBER OSIGURANJA?

Piše:
Zlata Dimić Ješić,
direktor za tehniku neživotnih osiguranja,
Generali osiguranje Srbija

U hiperpovezanom digitalnom svetu, sajber napadi pogađaju sve sektore. Tokom 2024. najčešće mete bili su: javna uprava (19%), transport (11%), finansije (9%), digitalna infrastruktura (8%).
Najzastupljenije pretnje bile su DDoS napadi, najviše usmereni na javni sektor (33%), transport (21%) i bankarstvo (12%).
Sajber rizicima nisu izložene samo kompanije – i pojedinci su meta. Više od 30% potrošača doživelo je neku vrstu sajber kriminala, dok je 14% bilo žrtva krađe identiteta.
U takvom okruženju, brza reakcija i efikasno ublažavanje posledica ključni su za očuvanje kontinuiteta poslovanja. Jedan od najpouzdanijih načina zaštite je – sajber osiguranje. Inovativna polisa sajber osiguranja Generali osiguranja Srbija kombinuje prevenciju, brzu reakciju i nadoknadu štete.

1. Prevencija i procena rizika
Kroz specijalizovanu platformu, klijentima je omogućeno skeniranje digitalnog perimetra, uključujući deep i dark web, kao i dobijanje izveštaja o sajber rizicima i potencijalnim pretnjama.

2. Reakcija na sajber napad
U saradnji sa ComTrade-om, klijentima je obezbeđena IT asistencija u slučaju incidenta – brza identifikacija, zaustavljanje napada i sprečavanje njegovog širenja. Prijava napada dostupna je 24/7 preko Generali kontakt centra.

3. Naknada štete kroz osiguranje
Polisa pokriva širok spektar troškova: obnavljanje podataka i softvera, usluge IT i pravnih eksperata, prekida poslovanja, zaštite reputacije, štetu na IT opremi, sajber ucene kao i odgovornost prema trećim licima zbog kršenja privatnosti i mrežne bezbednosti.
Limit pokrića se prilagođava profilu i potrebama svakog klijenta. Cena zavisi od veličine kompanije, delatnosti, stanja IT i internet bezbednosti, kombinacije pokrića i limita.

Na globalnom tržištu već postoje rešenja za lična sajber osiguranja koja nude:
- prevenciju
  (praćenje curenja podataka, zaštitu uređaja)
- zaštitu
  (nadoknadu štete od sajber prevare, iznude, phishinga)
- podršku (IT asistencija, pravna i psihološka pomoć)

Iako svest o sajber rizicima kod nas raste, potreba za osiguranjem još uvek nije dovoljno prepoznata. Zato industrija osiguranja radi na razradi rešenja za lično sajber osiguranje prilagođeno domaćem tržištu.
Sajber polisa nije samo osiguranje to je partner u sajber otpornosti vaše kompanije.

*Izvor podataka: ENISA Threat landscape 2024., Forrester Research|EuropAssistance – LexisResearch

« POVRATAK NA SADRŽAJ

AI U BANKARSTVU: IZMEĐU VEĆE SIGURNOSTI I NOVIH RIZIKA

Pišu:
Tatjana Grujičić
šefica Odeljenja za naprednu analitiku i upravljanje podacima rizika
Erste Banka Srbija

Vladimir Mićić
direktor Sektora za bezbednost
Erste Banka Srbija

U poslednjih nekoliko godina, zahvaljujući razvoju veštačke inteligencije (AI), bankarstvo prolazi kroz digitalnu transformaciju. Ogromna količina podataka koja se obrađuje i prikuplja svakog sata, uz sve veće zahteve za preciznom i odgovornom komunikacijom, kao i poštovanjem privatnosti klijenata, učinila je AI neophodnim saveznikom u automatizaciji, digitalizaciji i unapređenju poslovnih procesa. Jedan od ključnih koraka na tom putu je automatizacija manuelnih zadataka. Recimo, primena OCR (Optical Character Recognition) tehnologije zasnovane na AI omogućava automatsko učitavanje podataka sa dokumenata direktno u osnovni bankarski sistem ili baze podataka. Time se smanjuje mogućnost greške, ubrzava obrada i obezbeđuje kvalitetan unos podataka.
Primena savremenih tehnologija omogućava da se dugotrajni procesi koji zahtevaju dosta provera i razmenu informacija zamene brzim i efikasnim digitalnim rešenjima. Primera radi, apliciranje, odobravanje i isplata kredita putem bankarskih mobilnih aplikacija danas se mogu obaviti za samo nekoliko minuta bez odlaska u banku.
Modeli razvijeni upotrebom XGBoost, LightGBM, Random Forest i sličnih algoritama imaju za cilj da banka zadrži svoje klijente, ponudi im relevantne dodatne usluge i optimalno alocira svoje resurse. Sa druge strane, modeli treba da identifikuju klijente kojima je određena usluga zaista potrebna, kako bi komunikacija bila ciljana, korisna i nenametljiva, jer klijenti tada ne doživljavaju kontakt kao suvišan, već znaju da je banka efikasna i prisutna kad je zaista potrebna.
Finansijsko zdravlje klijenta je prioritet Erste Banke, a poznavanje klijenata, individualni pristup i saveti kako da se prevaziđu određeni finansijski izazovi mogući su jedino kroz detaljnu analizu podataka o klijentima i njihovim finansijskim aktivnostima. U svakom satu obrađuju se hiljade transakcija koje je potrebno nadgledati i kontrolisati, što prevazilazi mogućnosti čoveka da sve isprati i pravovremeno reaguje.

Zbog toga se koriste modeli koji funkcionišu u realnom vremenu, odmah nakon izvršenja transakcije, aktivirajući signal ukoliko prepoznaju nepoželjne obrasce.

Procedure su neizostavni deo bankarskog sistema, od onih koje propisuje regulator, preko internih procedura za korišćenje bankarskih sistema i procesa, do procedura koje su direktno vezane za potrebe klijenata. Chat botovi zasnovani na LLM (Large Language Model) su naši privatni i poslovni asistenti, koji nam olakšavaju pretrage, tumačenje procedura, pomažu u pisanju teksta, organizaciji posla, pravljenju prezentacija – ali svakako mogu da

budu ponuđeni i klijentima kao podrška 24/7, asistenti pri apliciranju za kredit ili analizi sopstvenih transakcija.

TREBA LI DA SE PLAŠIMO AI?

Gledano iz ugla bezbednosti, ključno pitanje glasi – treba li da se plašimo AI? Odgovor je svakako ne. Treba li da koristimo AI odgovorno, u skladu sa etikom i najboljim društvenim i poslovnim praksama? Svakako da.

Iz ugla upravljanja rizicima u bankama, AI se obično dovodi u vezu sa namernim ili nenamernim curenjem podataka i potencijalnim sajber napadima.

U tom procesu banke su neka vrsta dodatnog štita za klijente, jer vode računa računa o zaštiti njihovih sredstava i poverljivih informacija.

Sa novim alatima i servisima usavršavaće se i zaštitne mere. Banke nesumnjivo prednjače u primeni zaštitnih mehanizama i u zakonskom i u tehnološkom smislu, ali je ključno da ostanemo svesni granica u korišćenju veštačke inteligencije u bankarstvu. Dokle god ne delimo svoje lične podatke – jer oni treba da ostanu zaštićeni i isključivo naši – i dok AI koristimo kao podršku u procesu donošenja odluka, a ne kao zamenu za ljudski sud, prednosti su višestruke. Od bržih i preciznijih usluga, preko personalizovanih preporuka i lakšeg upravljanja finansijama, pa sve do unapređenja bezbednosti transakcija, potencijal je ogroman.

Istovremeno, rizici ostaju pod kontrolom, jer čovek zadržava ulogu onoga koji postavlja granice i donosi konačne odluke.

Na taj način, AI postaje saveznik – moćan alat koji bankarske usluge čini efikasnijim i dostupnijim, bez ugrožavanja poverenja i sigurnosti klijenata.

« POVRATAK NA SADRŽAJ

PRIMENA VEŠTAČKE INTELIGENCIJE U OSIGURANJU

Piše:
Maja Marković,
Marsh McLennan

U sektoru osiguranja i upravljanju rizicima, AI unosi novu dimenziju preciznosti, brzine i prediktivne analitike, pomažući kompanijama da budu spremnije za promene i otpornije na izazove.

Da ovaj trend prepoznaju i globalni lideri pokazuje najnovije istraživanje Oliver Wyman Foruma: čak 95% CEO lidera u svetu vidi AI kao priliku za svoju kompaniju, dok njih 17% već beleži rast prihoda ili smanjenje troškova za više od 10% zahvaljujući njenoj primeni.

Naravno, put nije bez izazova. Čak 41% CEO-ova smatra da je još rano za preciznu procenu povrata na ulaganje u AI. No, uprkos tome, pravac je jasan: većina lidera veruje da će upravo veštačka inteligencija oblikovati narednu deceniju poslovanja.

Štaviše, 71% CEO-ova ističe da najveći rizik ne leži u prevelikom oslanjaju na AI, već u tome da se sa njom ne radi dovoljno.

U Marsh McLennan-u verujemo da tehnologija nije tu da zameni ljude, već da ih osnaži, proširi njihove mogućnosti i otvori nova vrata. U okviru našeg globalnog ekosistema, koji okuplja Marsh, Guy Carpenter, Mercer i Oliver Wyman, AI postaje most između podataka i odluka.

Posebno bih izdvojila dva inovativna AI alata: LenAI, našeg internog asistenta za komunikaciju i podršku zaposlenima i Sentrisk, naprednu platformu za analitiku i upravljanje rizicima na način kakav dosad nije bio moguć.

LENAI – PAMETNI ASISTENT

LenAI je naš interni AI asistent osmišljen da zaposlenima olakša svakodnevni rad. Njegova glavna uloga je da ubrza pristup informacijama, pojednostavi procese i oslobodi vreme timovima kako bi se usredsredili na strateške ciljeve.

Zahvaljujući LenAI-ju, možemo mnogo brže da pronađemo relevantne podatke, pripremimo izveštaje, personalizovane ponude za klijenta, prezentacije ili poredimo ponude osiguravajućih društava. Rezultat su veća produktivnost i kvalitet usluge, uz značajno manje grešaka i manje utrošenog vremena na rutinske zadatke. Time se stvara prostor za ono što je najvažnije – kreativnost i izgradnju odnosa sa klijentima, a to je ono što tehnologija neće nikada moći da zameni.

LenAI je dragocen i u učenju. Može da kreira prilagođene materijale i simulacije, podržavajući kontinuirani profesionalni razvoj zaposlenih.

SENTRISK – INTELIGENTNA PLATFORMA ZA UPRAVLJANJE RIZICIMA

Sentrisk je razvijen da kompanijama širom sveta pruži naprednu analitiku i dubinsko razumevanje rizika. Nastao je iz sinergije Marsh-a i Oliver Wyman-a. Marsh donosi više od 150 godina iskustva u osiguranju i upravljanju rizicima, a Oliver Wyman

vrhunsku ekspertizu u strateškom konsaltingu i analitici.
Sentrisk kombinuje podatke iz javnih i privatnih izvora, napredne geoprostorne analize, AI algoritme i stručna znanja kako bi kompanijama omogućio da proaktivno prepoznaju i ublaže rizike. Platforma pruža end-to-end podršku upravljanju rizicima, što znači da ne samo da identifikuje probleme, već pomaže i u planiranju strategija, donošenju odluka i optimizaciji osiguravajućih rešenja. Platforma omogućava kompanijama da razumeju rizike u svojim lancima snabdevanja, prate dobavljače na svim nivoima i dobijaju real-time upozorenja o potencijalnim poremećajima i pretnjama.

Sentrisk je brzo stekao reputaciju lidera u svojoj oblasti i već je nagrađen na globalnom nivou - AXCO Global Insurance Awards 2025 proglasio ga je najboljom digitalnom inicijativom u osiguranju, dok ga je Business Insurance Innovation Awards 2024 izdvojio kao jedno od najinovativnijih rešenja na tržištu.
Da zaključim, alati kao što su LenAI i Sentrisk omogućavaju Marsh McLennan-u da bude agilniji, inovativniji i otporniji na izazove tržištu. Naši klijenti u Srbiji i svetu već osećaju benefite – brže donošenje odluka, proaktivno prepoznavanje rizika, optimizaciju svojih osiguravajućih pokrića. Naša misija ostaje ista – Know More. Do More.

« POVRATAK NA SADRŽAJ

KAKO AI UNAPREĐUJE NEPROFITNI SEKTOR I NJIHOVU PODRŠKU GRAĐANIMA

Piše:
HELVETAS

Ako u vremenu veštačke inteligencije, digitalizacije, radite sa građanima, ugroženim socijalnim grupama, onda radite sve da im omogućite bolji pristup informacijama i snalaženja u sistemu zarad ostvarivanja njihovih osnovnih prava. Rado biste razvili sistem brže i jednostavnije komunikacije sa zajednicom koja treba da se okupi i mobiliše radi rešavanja nekog ekološkog, društvenog problema ili promene neke regulative, ali niste sigurni kako.

To je slučaj i sa 30 partnerskih udruženja građana sa kojima *Helvetas Swiss Intercooperation* i „Građanske inicijative" sarađuju u okviru AKT projekta. To su udruženja koja deluju širom Srbije i svaka se u svom domenu bavi rešavanjem određenog problema – čistiji vazduh, bolja zdravstvena zaštita, stvaranje jednakih uslova za decu sa retkim bolestima, podrška ženama iz ruralnih područja, podrška parovima u procesu vantelesne oplodnje.

Međutim, udruženja slabo barataju digitalnim alatima u svakodnevnom radu, dok AI koriste u minimalnoj meri.

Srbija je inače na 57. mestu u svetu po indeksu spremnosti za veštačku inteligenciju i pozicionira se kao regionalni lider u odgovornom razvoju veštačke inteligencije.

Da li verujete da neke od ovih udruženja svoju bazu podrške čuvaju u sveskama? Uspešni u svojim poduhvatima, a koliko bi bili efikasniji da su digitalizovani?

Naša misija je da podržimo udruženja građana u Srbiji da postanu uticajni lideri i pokretači promena, zaista povezani sa svojim lokalnim zajednicama. Da bismo to ostvarili ponudili smo im mentorstvo i obuke iz oblasti *customer relationship management-a (*CRM-a), komunikacija, prikupljanja sredstava.

Neophodna promena u njihovom načinu rada bila je digitalizacija, i primena sistema CRM platformi koje se često sreću u privatnom sektoru u domenu prodaje, ali su za njih dizajnirane tako da mogu lako da formiraju bazu podrške, šalju mejlove, biltene, prate donacije, volonterske aktivnosti i sate, pripremaju i šalju izveštaje za donatore, prate potvrde prisustva na događajima, organizuju digitalne kampanje i njihovo praćenje. Ovakvo digitalno organizovanje podataka omogućava udruženjima da izgrade čvršće odnose, mere uticaj i poboljšaju strategije prikupljanja sredstava. Upotreba veštačke inteligencije u okviru CRM platformi i dalje je na niskom niovu. Međutim, uzimajući u obzir sa kojim korisnicima i građanima rade i koga zastupaju, udruženja građana moraju da budu izuzetno pažljiva u prikupljanju i čuvanju njihovih podataka. Uz primenu platforme, neophodan je etički princip upotrebe i zaštite podataka. CRM platforme koje koriste udruženja građana bi trebalo da primenjuju sledeće principe:

- **Transparentnost u prikupljanju podataka** – pružanje jasnih informacija o tome koji podaci se prikupljaju, zašto, kako se koriste i koliko dugo se čuvaju.
- **Saglasnost i opcije za odustajanje** – prikupljanje podataka mora biti uz eksplicitnu saglasnost korisnika, uz mogućnost da se ta saglasnost povuče u bilo kom trenutku.
- **Bezbednost podataka** – CRM mora da koristi enkripciju, višefaktorsku autentifikaciju i redovne bezbednosne provere kako bi sprečio neovlašćen pristup.
- **Pravo na pristup i ispravku** – korisnici imaju pravo da vide koje podatke udruženja građana poseduju o njima i da ih isprave ako su netačni.
- **Ograničenje svrhe i trajanja čuvanja** – podaci se smeju koristiti samo za svrhu za koju su prikupljeni i ne smeju se čuvati duže nego što je potrebno.

« POVRATAK NA SADRŽAJ

BE
RISK
PROTECTED.

AKO IMATE ŠTA DA KAŽETE NA TEMU
- RIZIKA
- BEZBEDNOSTI
- ODRŽIVOG POSLOVANJA

UKLJUČITE SE U
NAŠE AKTIVNOSTI

Specijalna
godišnja edicija
„MOĆ ODRŽIVOG
POSLOVANJA“
10. mart 2026.

Godišnja konferencija
„RIZICI NOVOG DOBA“
4. jun 2026.
Hotel Hilton Beograd

Budite deo aktivne i napredne grupe poslovnih ljudi, koja želi da doprinese bezbednijem društvu i poslovanju u doba rastućih rizika.

DIGITALNA DEMENCIJA I DIGITALNI MINIMALIZAM

Piše:
Vojislav Rodić,
CEO **I Net**

„Digitalna demencija“ nije kodifikovana medicinska dijagnoza (mada zvuči autentično). Radi se o naslovu knjige koju je 2012. objavio nemački naučnik Manfred Špicer. Od tada je taj izraz „ušao u stručni narod“ pa ga koriste i kliničari i mediji kada opisuju simptome opadajućih kognitivnih sposobnosti kod onih koji intenzivno koriste digitalne tehnologije, a posebno kod mladih. Najčešće se problemi manifestuju kao slabije pamćenje, skraćen raspon pažnje, umanjene spoznajne kao i sposobnosti društvene interakcije. Zaboravljaju se imena, brojevi telefona, zakazane obaveze, oslabljena je mogućnost koncentracije i rešavanja problema, a uočljiva je i uzdržanost u društvenim kontaktima.

ŠTA SU MOGUĆI UZROCI OVIH PROBLEMA?

Digitalni alati nam olakšavaju aktivnosti povezane sa pamćenjem, ali i prostornom i društvenom orijentacijom. Ako se te aktivnosti izmeštaju iz vas u vaše uređaje, vaše sposobnosti se smanjuju jer se manje koriste. Stalni „multitasking“ između aplikacija, notifikacija, listanja beskrajnih strana na internet platformama nas uvodi u stanje „plitke“ obrade informacija, dok je za dugotrajno pamćenje i rešavanje problema neophodna duboka koncentracija. Ne treba zaboraviti ni dugotrajno izlaganje plavom svetlu ekrana, koje ima izuzetno negativne efekte po kvalitet sna, a dobar san je neophodan za konsolidaciju našeg pamćenja. Na kraju, i samo vreme koje provodimo nad ekranima je oduzeto od drugih aktivnosti – od onih povezanih sa fizičkim kretanjem do onih koje čine potku naših društvenih veza.

„Digitalna demencija“ ne izaziva trajno oštećenje mozga (kao Alchajmerov sindrom) iako neki od simptoma slično izgledaju. Korekcije u korišćenju digitalnih tehnologija mogu da dovedu do poboljšanja stanja, posebno ako se usvoje i zdrave navike: kretanje, cirkadijalni ritam budnog stanja i sna, umerena ishrana.

KAKO ZAŠTITITI SEBE I DECU OD TOG RIZIKA?

Digitalni alati koje danas nazivamo „veštačkom inteligencijom“ samo su grube aproksimacije misaonih procesa, ali i takvi mogu da pruže kvalitetne odgovore onima koji znaju šta traže, kao i šta da očekuju - pod uslovom da pažljivo motre da njihov AI alat ne odluta u povremene halucinacije.

Direktor firme OpenAi, Sem Altman je polovinom 2025. izjavio: „Ljudi imaju veoma visok nivo poverenja u ChatGPT, što je zanimljivo jer AI haluicinira. To je tehnološki proizvod kojem ne bi trebalo previše da verujete“. Ako nam jedan od autora poručuje da je jedan od vodećih botova AI nepouzdan u svojim odgovorima, onda bi to već trebalo da bude dovoljan razlog za našu uzdržanost.

Neke zemlje uvode ograničavanje korišćenja tzv. društvenih mreža ispod određene starosne granice (14, 12 godina) bilo potpunom zabranom (Australija) ili dnevnim ograničenjima. TikTok (Bajdu) za korisnike u Kini ispod 12 godina ima ugrađeno ograničenje od 45 minuta dnevno u periodu 06-22, dok američki tinejdžeri na toj aplikaciji (za američko tržište) provode 6-8 sati dnevno. Što su mlađi to više vremena odvajaju za hipnotišuće kratke video forme.

Zabrane mogu da pomognu samo ako su istovremeno praćene ispunjavanjem „oslobođenog" vremena drugim aktivnostima. U porodici to podrazumeva da se roditelji više bave decom, da pričaju sa njima, i da ih slušaju, da ih upoznaju i usmeravaju njihovo ponašanje (to se nekad zvalo „vaspitanje").

U korišćenju digitalnih tehnologija cilj je ponašanje koje možemo da nazovemo „digitalni minimalizam" – to nije odustajanje od tehnologije, već njeno smisleno i usmereno korišćenje u meri koja je proporcionalna željenom efektu. Ovako napisano – deluje lako ostvarivo, ali imajte na umu da se borite protiv timova najboljih psihologa i sociologa koji su sve svoje talente stavili u službu jednog cilja – da vas zadrže što duže pred magičnim ekranom kojem poveravate svoja najintimnija opredeljenja i uverenja. Možete da budete poslušni podanik ekranokratske elite ili digitalni pobunjenik, koji će koristiti najmodernije tehnologije u svoju korist. Na kraju sve zavisi samo od vas i vaše slobodne volje.

Ceo tekst pročitajte **OVDE**.

« POVRATAK NA SADRŽAJ

KUPUJEMO KOMFOR, PRODAJEMO INTIMU

Piše:
Nastasija Maksimović,
AI inženjer

Istraživanja pokazuju da samo trećina ljudi misli da koristi AI, dok ga zapravo koristi više od dve trećine. Mnoge „životne udobnosti“ prihvatamo zdravo za gotovo, i ne znajući da iza mogućnosti koje nam razne sprave oko nas pružaju zapravo stoji veštačka inteligencija. Ipak, mnogo je razloga da postavimo pitanje: gde je granica?
Prvi AI algoritmi osmišljeni su pre nekoliko decenija, i koristimo ih ne razmišljajući o njima jer su „nevidljivi“, odnosno rade u pozadini: filteri za spam štite naše mejlove, Google mape uče gde su gužve u saobraćaju, Netflix i Spotify prilagođavaju svoje preporuke na osnovu našeg ponašanja.
Na primer, Google mape ne znaju da je gužva jer je neko „ručno“ prijavljuje, nego zato što algoritmi prate naše kretanje: ako na određenom mestu svi naglo uspore, AI prepoznaje zastoj i predlaže obilaznicu. Netflix ne nudi naslove nasumično, nego prati ne samo šta smo pogledali, već i gde smo pauzirali, koje scene preskačemo i koliko brzo odustajemo od serija i filmova. Spotify analizira vreme dana, brzinu, žanr, tempo, energiju pesama koje slušamo i kombinuje to sa ponašanjem miliona drugih korisnika kako bi pogodio šta nam se baš sada sluša.
Vremenom, došli smo do toga da je danas AI postao "vidljiv". Veliki jezički modeli, kao što je ChatGPT, omogućili su nam da razgovaramo sa mašinama ljudskim jezikom kao sa prijateljima. Oni to rade toliko uverljivo da ljudi počinju slepo da im veruju. U praksi, to poverenje zna da bude opasno. U Americi je zabeležen slučaj tinejdžera koji je razgovarao sa AI chatbotom, počeo da izražava suicidne misli, AI ga je ohrabrivao u tome, i nedugo zatim dečak je oduzeo sebi život.
Ali upravo ta uverljivost i osećaj koji razgovor sa mašnama uspeva da probudi u ljudima razlog je zašto je AI postao toliki trend. Zato ga sada želimo svuda: u frižideru, četkici za zube, pa čak i u toaletu. Ali, da li nam je stvarno potreban baš u svakoj sferi života?

GDE JE GRANICA?

I tu se otvara pitanje – gde je granica? AI je koristan kada nam olakšava rad, štiti od prevara ili ubrzava procese. Ali sve se češće pitamo – da li je AI zaista svuda neophodan?

Rutinski zadaci nisu samo posao; oni su trenuci introspekcije i osećaj da nešto sami činimo. Kada AI sve to preuzme, gubimo deo svoje autonomije i identiteta.

Postoji krilatica: "Želim da AI pere moj veš i sudove kako bih ja mogla da se bavim pisanjem i umetnošću, a ne da AI piše i stvara umetnost dok ja perem veš." Ali realnost

je često drugačija: AI već pomaže u domaćinstvu, a istovremeno piše naše mejlove i kreira slike.
Postoje i naučni dokazi da AI menja naš način razmišljanja. Istraživanja pokazuju da predlozi naredne reči ili fraze (next-word suggestions) čine naše pisanje predvidljivijim i kraćim, ali što je najvažnije - drugačijim od onoga što bismo mi rekli. AI ne menja samo ono što pišemo, već i način na koji odlučujemo ili - odlučuje umesto nas.
I dok mi razmišljamo o tome, AI je već svuda oko nas. AI robot Flippy priprema hamburgere u restoranima; aplikacija u Japanu predviđa bol kod mačaka na osnovu fotografija; algoritmi kreiraju parfeme i viski analizirajući milione kombinacija. Sve ovo su aktivnosti koje bi trebalo da pričinjavaju zadovoljstvo i značenje našem danu. Sve to pokazuje koliko je AI "lepljiv" i koliko brzo može da uđe u naše živote - ponekad korisno, a ponekad potpuno ludo.

PRIVREMENO JEFTIN, TRAJNO SKUP

Još jedan sloj priče je ekonomski. Danas je AI jeftin ili besplatan jer je trend. Velike kompanije ulažu milijarde da bismo se navikli na njega, ali jednom kada postane neizostavan, cena će porasti, u valuti novca i privatnosti. Setimo se da je i Uber bio jeftin dok nam nije postao potreba, a zatim podigao cene.
Prodajemo li deo svoje intime za trenutni komfor? I da li nam preterani komfor čini magareću uslugu? Frižider zna šta jedemo, telefon gde idemo, aplikacije kada spavamo. Mi dobijamo personalizovane preporuke, a kompanije dobijaju nas.

« POVRATAK NA SADRŽAJ

PAMETNI GRADOVI VIŠE NISU “SF”

Nekada zamišljeni kao scene iz naučnofantastičnih filmova, pametni gradovi danas postaju realnost: tehnologija je toliko odmakla da su pojedini urbani centri pretvoreni u „laboratorije održivosti“, efikasnosti i digitalnih usluga. Ipak, izgleda da se dosta vodi računa o tome da se primenjuju rešenja koja mogu da vide i osete najpre obični građani.

Primera radi, u Singapuru postoje semafori koji sami produžavaju zeleno svetlo kada detektuju da stariji pešak prelazi ulicu sporije. Amsterdam koristi pametne kontejnere koji šalju signal komunalnim službama kada se napune, pa kamioni ne kruže bespotrebno. U Kopenhagenu, deo ulične rasvete je povezan na senzore pokreta – svetla se prigušuju kada nema nikoga, a jače svetle kad naiđe biciklista ili pešak. Zahvaljujući tome gužve su manje, štedi se energija a vazduh je čistiji.

ŠTA JE NAJVAŽNIJE, A ŠTA NAJBRŽE NAPREDUJE

Jedna od najvažnijih oblasti su pametne električne mreže. U Tokiju i Seulu sistemi automatski preusmeravaju struju tamo gde je najpotrebnija - zgrade sa solarnim panelima vraćaju višak energije u mrežu, pa građani postaju i potrošači i proizvođači struje. Na ovaj način smanjuje se zavisnost od fosilnih goriva i čuva životna sredina.

Glavni fokus je i dalje na saobraćaju koji najdirektnije utiče na svakodnevicu. Pametni autobusi u Helsinkiju povezuju se sa mobilnim aplikacijama i obaveštavaju putnike kada tačno stižu na stanicu. U Dubaiju testiraju taksi-dronove za prevoz putnika. U nekim gradovima, poput Los Anđelesa, aplikacije povezuju više vrsta prevoza – metro, bicikle i taksi – kako bi građani dobili najbržu i najjeftiniju rutu u jednom potezu.

Pored saobraćaja, sve više pažnje dobija i pametno upravljanje vodom. Senzori u kanalizaciji u Kopenhagenu upozoravaju na moguću poplavu, dok u Indiji postoje sistemi koji kontrolišu gubitke vode u cevima i sprečavaju nestanke.

METAVERZUM I VIRTUELNA REALNOST

Jedan od najnovijih trendova je upotreba VR-a i metaverzuma u planiranju gradova. Umesto crteža na papiru, urbanisti “ulaze” u virtuelne modele i hodaju budućim ulicama. Na taj način mogu da testiraju koliko će park zaista biti osunčan ili da li će nova raskrsnica

napraviti saobraćajni čep. U Japanu se VR koristi čak i za simulaciju evakuacije tokom zemljotresa, kako bi se unapred uočile slabosti u planovima.

Iako Srbija ne spada u pionire, i kod nas se polako pojavljuju pametna rešenja.

Beograd i Novi Sad uvode sisteme za pametne parkinge, a Niš modernizuje javnu rasvetu kroz javno-privatno partnerstvo, i za taj projekat dobio je nagradu Ambasade Francuske kao „Ekoopština". U tom gradu u planu je zamena oko 23.000 starih svetiljki LED tehnologijom i uvođenje pametnih sistema upravljanja, što će obezbediti oko 73 odsto garantovane uštede (do 120 miliona dinara manje troškova godišnje). Građani će dobiti ravnomernije i bezbednije osvetljene ulice, parkove i staze, uz manju potrošnju energije i čistiju životnu sredinu.
Veća integracija podrazumevala bi povezivanje saobraćaja, ekologije i energetike – tada bi u Srbiji, kao na primer u Aziji i zapadnoj Evropi - pametni gradovi postali deo svakodnevnog života.

UVEK IMA NEKO „ALI"...

Ovi sistemi prikupljaju ogromne količine podataka o građanima, pa se tu ozbiljno otvara pitanje privatnosti jer kamere koje prate saobraćaj ili senzori koji mere potrošnju struje zapravo beleže navike građana. Zato je ključno da gradovi uvode pravila zaštite podataka i da se informacije o građanima drže anonimnim. Evropska unija insistira na tome, dok zemlje poput Kine idu u smeru mnogo šireg nadzora – što otvara dilemu gde je granica između sigurnosti i slobode.

Baš kao "živi organizmi", pametni gradovi praktično sami reaguju na promene, bilo da je reč o gužvi na autoputu, poplavi ili nestašici struje.

To za građane znači manje čekanja, čistiji vazduh i efikasnije usluge. Ali – jedan od najvažnijih zadataka za one koji tehnologijama barataju jeste da ih primenjuju odgovorno – i ovo nije samo fraza, jer u suprotnom će se umesto humanije sredine prilagođene ljudima, oni pretvoriti hladne robotske tvorevine.

« POVRATAK NA SADRŽAJ